Washington Law Review

Volume 95 | Number 1

3-2020

Privacy as Safety

A. Michael Froomkin
University of Miami School of Law, froomkin@law.miami.edu

Zak Colangelo
Zak.Colangelo-Trenner@lewisbrisbois.com

PRIVACY AS SAFETY

Michael Froomkin[*] & Zak Colangelo[**]

Abstract: The idea that privacy makes you safer is unjustly neglected: public officials emphasize the dangers of privacy while contemporary privacy theorists acknowledge that privacy may have safety implications but hardly dwell on the point. We argue that this lack of emphasis is a substantive and strategic error and seek to rectify it. This refocusing is particularly timely given the proliferation of new and invasive technologies for the home and for consumer use more generally, not to mention surveillance technologies such as so-called smart cities.

Indeed, we argue—perhaps for the first time in modern conversations about privacy—that in many cases privacy is safety, and that, in practice, United States law already recognizes this fact. Although the connection rarely figures in contemporary conversations about privacy, the relationship is implicitly recognized in a substantial but diverse body of U.S. law that protects privacy as a direct means of protecting safety. As evidence we offer a survey of the ways in which U.S. law already recognizes that privacy is safety, or at least that privacy enhances safety. Following modern reformulations of Alan Westin's four zones of privacy, we explore the safety-enhancing privacy protections within the personal, intimate, semi-private, and public zones of life, and find examples in each zone, although cases in which privacy protects physical safety seem particularly frequent. We close by noting that new technologies such as the Internet of Things and connected cars create privacy gaps that can endanger their users' safety, suggesting the need for new safety-enhancing privacy rules in these areas.

By emphasizing the deep connection between privacy and safety, we seek to lay a foundation for planned future work arguing that U.S. administrative agencies with a safety mission should make privacy protection one of their goals.

---

[*] Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law, University of Miami, Fellow Yale Information Society Project, Member Miami Center for Computational Science. We would like to thank Caroline Bradley, David Froomkin, Bert-Jaap Koops, Charles Raab, Jonathan Weinberg, and participants at the 2018 Amsterdam Privacy Conference session on Socializations and the Value of Privacy for helpful comments. We are grateful to Phillip Arencibia, Gil Greber, Nicholas Mignanelli and Robin Schard for help with research.

[**] Attorney, Lewis Brisbois Bisgaard & Smith LLP, Coral Gables, Florida.

INTRODUCTION

In this Article we seek to forefront a longstanding justification for privacy: that it makes you safer. We do so for three reasons.

First, privacy is too often attacked on the grounds that it grants terrorists and criminals the ability to put people in harm's way.[1] We do not, in this

1. The law-enforcement argument is exemplified by the testimony of an FBI representative to Congress:

> In order to better protect this nation and its people from harm, we need to be able to access electronic information . . . [or else] we may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our

Article, analyze the strength of claims that privacy may be harmful. Rather, we seek to balance the discussion by pointing out that privacy is a two-way street, in that it also protects people from many dangers, and that (primarily U.S.) law and official practices already reflect this understanding in a variety of ways. We believe that this reminder is particularly timely given the proliferation of new and invasive technologies for the home and for consumer use more generally, not to mention surveillance technologies such as so-called smart cities.[2]

> neighborhoods. We may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence.

Statement Before the House Committee on Energy and Commerce, Subcomm. on Oversight and Investigation, 114th Cong. (2016) (statement of Amy Hess, Executive Assistant Director, Science and Technology Branch Federal Bureau of Investigation), https://www.fbi.gov/news/testimony/deciphering-the-debate-over-encryption [https://perma.cc/3YWB-NJVB]; *see also* STEWART BAKER, SKATING ON STILTS (2010).

Other arguments rest on the need to prevent the use of information communication technologies to silence or harm women and other vulnerable groups. *See* DANIELLE K. CITRON, HATE CRIMES IN CYBERSPACE (2014); Danielle K. Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401 (2017); Mary A. Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655 (2012) (proposing liability on intermediaries so they will identify or discipline bad actors); Erin Peebles, *Cyberbullying: Hiding Behind the Screen*, 19(10) PEDIATRICS & CHILD HEALTH 527 (2014)

Justice Scalia, himself at times a defender of privacy, summed up the case against anonymity, a strong form of privacy, in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). Anonymity, he wrote, is generally dishonorable: "It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity." *Id.* at 385 (Scalia, J., dissenting). To create legal protection for anonymous communication absent a reason to expect "threats, harassment, or reprisals," he argued, "seems to me a distortion of the past that will lead to a coarsening of the future." *Id.*

2. A "smart city" is a "data-driven city [that] depends on data collected from buildings, infrastructure, people, and third-party data brokers. Government agencies, quasi-governmental utilities, commercial interests, and others will trace, analyze, and predict the movements, needs, and scarcities of citizens in the city in order to manage resources and protect the community most effectively." Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309, 311 (2017). Commonly, the monitoring devices will include components of the so-called "Internet of Things." *See* Jesse W. Woo, *Smart Cities Pose Privacy Risks and Other Problems, but That Doesn't Mean We Shouldn't Build Them*, 85 UMKC L. REV. 953, 955 (2017). The result, in either case, is "ubiquitous surveillance." Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1582 (2014). For discussion of some of the privacy issues raised by extensive data collection in smart cities, see ALVARO ARTIGAS, INSTITUT BARCELONA D'ESTUDIS INTERNACIONALS, SURVEILLANCE, SMART TECHNOLOGIES AND THE DEVELOPMENT OF SAFE CITY SOLUTIONS: THE CASE OF CHINESE ICT FIRMS AND THEIR INTERNATIONAL EXPANSION TO EMERGING MARKETS 1 (2017), https://www.ibei.org/surveillance-smart-technologies-and-the-development-of-safe-city-solutions-the-case-of-chinese-ict-firms-and-their-international-expansion-to-emerging-markets_112561.pdf [https://perma.cc/CP8X-477M]; THEO BASS, EMMA SUTHERLAND & TOM SYMONS, DECODE, RECLAIMING THE SMART CITY PERSONAL DATA, TRUST AND THE NEW COMMONS (2018), https://media.nesta.org.uk/documents/DECODE-2018_report-smart-cities.pdf [https://perma.cc/7LJZ-X2BR]; Finch & Tene, *supra* note 2. A somewhat more positive account appears in Woo, *supra* note 2.

Second, the current—and understandable—focus on the data-protection strand of privacy protection (which focuses on the how) threatens to obscure other worthy justifications for privacy (the why). That privacy enhances safety is, most certainly, not a new idea. But, with the possible exception of debates over electronic privacy, concepts of safety tend not to figure centrally in contemporary conversations about privacy. With the coming of smart cities and other types of mass surveillance in the physical and electronic realms, however, personal privacy is threatened as never before.[3] It is time, therefore, for some modern threat analysis: in what ways are people put in danger—physically, economically, politically—by having others within the private or public sectors know things about them? We seek to rescue this aspect of the privacy pantheon from its slide into relative obscurity.

Third, we seek to lay a foundation for future work[4] showing how—if privacy is indeed a form of safety—it follows that a number of U.S. administrative agencies charged with ensuring various aspects of public safety have a heretofore unacknowledged duty to consider privacy issues when crafting their regulations.[5]

Demonstrating that privacy is actually a form of safety will, in turn, open the door for future U.S. administrative-law arguments that federal agencies with safety missions—including the Federal Aviation Administration,[6] the Consumer Product Safety Commission,[7] and the Food and Drug Administration[8]—are legally obligated to consider privacy consequences when drafting safety rules that directly or indirectly affect privacy.[9] Drawing attention to the ways in which privacy enhances safety

3. *See infra* section III.B.2, Part IV.

4. Tentatively titled "Safety as Privacy."

5. In the United States, there are a number of agencies with statutory obligations to protect public safety in various ways. For example, the U.S. Federal Aviation Administration (FAA) is charged with protecting public safety in air transportation. In crafting rules for the regulation of unmanned aerial vehicles (UAVs), commonly known as drones, the FAA has consistently taken the position that its safety mandate is limited to physical safety and does not require—if indeed it even permits—consideration of the privacy-related consequences of UAV usage. *See, e.g.*, Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552–53 (Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, and 183).

6. *See, e.g.*, 49 U.S.C. § 40104 (2012) ("The Administrator of the Federal Aviation Administration shall encourage the development of civil aeronautics and safety of air commerce in and outside the United States.").

7. *See* Griswold Insulation Co. v. Lula Cotton Processing Co., 540 F. Supp. 1334, 1339 (M.D. Tenn. 1982) (holding that economic injury is in the scope of Consumer Product Safety Commission (CPSC) regulation, as the statutory term "risk of injury" is not limited to physical injury).

8. *See, e.g.*, 21 U.S.C. § 393 (2012) (requiring FDA to ensure that "there is reasonable assurance of the safety and effectiveness of [regulated] devices intended for human use").

9. The court declined to reach this issue in *Electronic Privacy Information Center v. Federal Aviation Administration*, 892 F.3d 1249 (D.C. Cir. 2018).

should lead more routinely to treating privacy as a legitimate object of safety agendas. This instrumental goal (not to mention our own parochial limitations) explains the U.S.-centric approach in what follows.

This Article proceeds in four Parts. It begins by offering working definitions of two key terms: "privacy" and "safety." The second Part looks at contemporary privacy theory and offers some justifications for our claim that the safety value of privacy plays only a very small role. The third and longest Part turns from theory to practice, and provides a catalog of rules and circumstances in which the U.S. legal system explicitly or implicitly recognizes the importance of privacy as a means of achieving safety. The fourth Part identifies certain technological (and in one case social) innovations that threaten privacy and in so doing undermine safety; to the extent that these innovations are susceptible to regulation, it likely follows that making rules to protect personal privacy would make people safer.

The Article concludes that both theoretical discussions of privacy and practical attempts to make both safety-enhancing and privacy-enhancing policies would benefit from taking fuller account of the important role that privacy can play in making us safe.

I. TWO DEFINITIONS

A. Privacy

Privacy is a notoriously protean concept. It is social.[10] It is multifarious.[11] It is sometimes said to be incoherent.[12] If judged solely by

10. *See* BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 73 (1984).

11. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

12. *See* Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 1 (2019) ("The problem of theorizing privacy moves on two levels, the first consisting of an inadequate conceptual vocabulary and the second consisting of an inadequate institutional grammar. Theories about privacy have a tendency to dissolve into contradictions. So, for example, one justification commonly asserted for privacy is that it promotes and protects individual autonomy, but making privacy serve autonomy effectively is impossible unless one confronts the constructedness of selfhood. Another common justification for privacy is that it promotes and protects an essential degree of separation between self and society. That justification is implicitly predicated on the reality of social construction, but making privacy serve the construction of selfhood effectively is impossible unless one confronts privacy's social (i.e., collective) value."); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088—89 (2002) (footnotes omitted) ("Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy. Arthur Miller has declared that privacy is 'difficult to define because it is exasperatingly vague and evanescent.' According to Julie Inness, the legal and philosophical discourse of privacy is in a state of 'chaos.' Alan Westin has stated that '[f]ew values so fundamental to society as privacy have been left so undefined in social theory . . . .' William Beaney has noted that

the volume of academic writing today, though, privacy is about data protection.[13] This is only natural: due to rapid technical change, informational privacy is the fastest-shriveling portion of the privacy landscape. It is the area where, thanks largely to the European Union's General Data Protection Regulation (GDPR),[14] we see the most legal ferment.

Privacy theorists' focus on informational privacy crowds out the safety-enhancing aspects of privacy from contemporary conversations even though it is common to state that privacy is important to allow human flourishing.[15] For example, Julie Cohen sees privacy as necessary to "the

---

'even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right.' Privacy has 'a protean capacity to be all things to all lawyers,' Tom Gerety has observed. According to Robert Post, '[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.' Several theorists have surveyed the interests that the law protects under the rubric of privacy and have concluded that they are distinct and unrelated. Judith Thompson has even argued that privacy as a concept serves no useful function, for what we call privacy really amounts to a set of other more primary interests.").

13. *See* Bert-Jaap Koops et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483, 487–88 (2017) (noting "the trend, visible since the 1960s, to focus predominantly on informational privacy and data protection").

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L [2016] 119/1 at Arts. 17, 21 [hereinafter GDPR].

15. A few examples are FERDINAND D. SCHOEMAN, PRIVACY AND SOCIAL FREEDOM 22 (1992) (stating privacy "protect[s] individuals from the overreaching control of others"); Chris Clark, *Against Confidentiality? Privacy, Safety and the Public Good in Professional Communications*, 6(2) J. SOC. WORK 117, 124 (2006) ("[T]he *point* of privacy-as-seclusion is . . . that it serves to protect the sphere of the private-as-non-public. Without protection of the private-as-non-public the way is open to fascism and other sorts of totalitarianism."); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 1006—07 (1996) (arguing that "[t]houghts and opinions, which are the predicates to speech, cannot arise in a vacuum," and a right to read anonymously is necessary for the "iterative process of 'speech-formation—which determines, ultimately, both the content of one's speech and the particular viewpoint one espouses"); H. Tristram Engelhardt, Jr., *Privacy and Limited Democracy: The Moral Centrality of Persons,* 17(2) SOC. PHIL. & POL'Y 120 (2000) (noting that rights to privacy mark where individuals continue to maintain authority over themselves); Daniel E. Newman, *European Union and United States Personal Information Privacy, and Human Rights Philosophy - Is There a Match*, 22 TEMP. INT'L & COMP. L.J. 307, 312 (2008) ("If a person is unable to control access to personal information about herself, then she may be subjected to unwanted social pressures to conform to norms that she may not otherwise wish to adopt."); *id.* at 315 ("Privacy, as interiority, is meant to preserve inner-reflection, which leads to outer, social good through the activity of a self-reflective, self-realized individual."); Jed Rubenfeld, *The Right to Privacy*, 102 HARV. L. REV. 737, 784 (1989) (arguing that core of right to privacy is the right to determine the course of one's own life); Elizabeth M. Schneider, *The Violence of Privacy*, 23 CONN. L. REV. 973, 979 (1991) (internal footnotes omitted) ("[Privacy] provides an opportunity for individual self-development, for individual decision making and for protection against endless caretaking. In addition, there are other related aspects of privacy, such as the notion of autonomy, equality, liberty, and freedom of bodily integrity, that are central to women's independence

liberal self's capacity for critical independence of thought and judgment, its commitments to self-actualization and reason, and its aspiration to cosmopolitanism" all of which she describes as "essential tools for identifying and pursuing the material and political conditions for self-fulfillment and more broadly for human flourishing."[16] "Privacy," agrees Ryan Calo, "is best understood as an instrument of human flourishing."[17] It is much less common—even in accounts that view privacy as a solely instrumental good—to discuss privacy as enhancing safety. This Article seeks to contribute to the development of privacy theory by filling that gap.

But before assessing the role of safety in privacy theory, it is helpful to provide, as context, an overview of certain significant and influential understandings or definitions of what "privacy" is and why it is important.

Scholars routinely lament the difficulty of defining "privacy." According to Daniel J. Solove, this definitional difficulty stems, in part, from an inability to see the forest for the trees.[18] Theorists have failed to develop a useful conception of the term, Solove argues, because they have generally "failed to adequately conceptualize the problems that privacy law is asked to redress."[19] Untethered to a notion of what privacy should do, scholars have been unable to say what it is.

1. Earlier Definitions of Privacy

Perhaps because of this difficulty, definitions of privacy can be very general. Famously, Louis Brandeis and Samuel Warren wrote that privacy is the "right to be let alone."[20] This fundamental insight remains one of the most cited and influential definitions of privacy in the past 100 years.

Another foundational conception of privacy traces to Alan Westin's 1967 book *Privacy and Freedom*. Westin understood privacy as a four-stage spectrum—solitude, intimacy, anonymity, and reserve—in which the individual's involvement with the public sphere increases at each

---

and well-being.").

16. Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1911 (2013).

17. Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649, 651 (2015) (citing Cohen, *supra* note 16).

18. Solove, *supra* note 12, at 1090.

19. *Id.*

20. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). *Cf.* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (writing that U.S. Constitution "conferred, as against the government, the right to be let alone–the most comprehensive of rights and the right most valued by civilized men").

stage.[21] Solitude is the most complete type of privacy that one can achieve. It is marked by isolation from other people, leaving one alone with one's thoughts.[22] Moving one step closer to the public sphere, intimacy refers to an individual's involvement in a small social circle: with spouses, partners, friends, families, or other close-knit communities like coworkers.[23] Anonymity exists where one resides in the public sphere but nevertheless avoids the focused attention of others.[24] This is a type of "public privacy," or privacy in public.[25] The final state—reserve—involves the erection of barriers to prevent others from accessing information about oneself.[26] These barriers may grow from the subject, as where one declines to share information, or from the discretion of the others, as where the individual relies on the restraint of others to avoid the sharing of the private.[27]

In contrast, Solove argues for a "pragmatic" approach to conceptualizing privacy, "focusing on the palpable consequences of [privacy] rather than on [its] correspondence to an ultimate reality."[28] In this way, Solove subscribes to philosopher John Dewey's view that "philosophical inquiry should begin as a response to dealing with life's problems and difficulties."[29] Specifically, Solove argues that "privacy" is best understood through Ludwig Wittgenstein's concept of "family resemblances."[30] The idea of "family resemblances" rejects the proposition that a concept—for example, privacy—can be defined through identification of universally applicable necessary and sufficient conditions, or "rigid conceptual boundaries and common denominators."[31] Thus rejecting the search for a term's essence, Wittgenstein instead looks to the "complicated network of similarities overlapping and crisscrossing."[32] Correspondingly, Solove suggests we

---

21. ALAN F. WESTIN, PRIVACY AS FREEDOM 31–32 (1967).

22. *Id.* at 31.

23. *Id.*

24. *Id.*

25. *Id.* at 32.

26. *Id.*

27. *Id.*

28. Solove, *supra* note 12, at 1091.

29. *Id.* at 1093 (citing JOHN DEWEY, LOGIC, THE THEORY OF INQUIRY 106–10 (Jo Ann Boydston ed., 1988)).

30. *Id.* at 1092, 1126–27.

31. *Id.* at 1126.

32. LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS, § 66, 27 (G.E.M. Anscombe trans., 1958).

look to pools of similarities and differences between different types or aspects of things that might be considered private. Solove himself looks to privacy "practices"—"activities, customs, norms, and traditions"[33]—to identify the manner in which the concept has developed as a matter of reality. To "define" the term, therefore, Solove focuses on "certain matters [that] Western societies have long understood as private: the family, the body, and the home."[34]

In this view, privacy is that collection of things that we consider private and that, in practice, are treated as private. It is a descriptivist approach, and it seeks to reflect commonsensical understandings of what is, or should be, private. The descriptivist approach, however, leads to another potential problem in defining "privacy": people's professed understanding of what is or should be private often does not track with their actions.[35] That is, while people say they want privacy, their actions often suggest otherwise.

Helen Nissenbaum seeks to resolve this seeming contradiction with her theory of privacy as contextual integrity.[36] Her approach to understanding privacy is analogous to tort law's focus on reasonableness. Heavily contextual, what might be private in one situation might not be private in another. A privacy violation, then, is not merely the sharing of given information, but the inappropriate sharing thereof—an inquiry that calls for an evaluation of context.[37] Nissenbaum's definition of privacy violations suggests that people are not, in the main, insincere or irrational when they state a preference for privacy but act in ways that seem to undermine that preference:

> If a right to privacy is a right to context-appropriate flows [of information], and not to secrecy or to control over information about oneself, there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information as long as the sharing and withholding conform with the principled conditions prescribed by governing contextual norms.[38]

---

33. *See* Solove, *supra* note 12, at 1092.

34. *Id.* at 1093.

35. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 104–08 (2010) (recognizing the "stark contradiction" between people's stated concern for privacy and their actions: "[i]n almost all situations in which people must choose between privacy and just about any other good, they choose the other good," for example, "credit cards over cash, E-ZPass over traditional toll payments, . . . traceable search engines over self-directed Web surfing").

36. *Id*.

37. *See id.* at 186–230.

38. *Id.* at 187.

Julie E. Cohen's definition of privacy is similar in the sense that it is dynamic, incapable of being reduced to a "fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic."[39] But while Nissenbaum defines privacy in relation to the full spectrum of possible contexts, Cohen's approach is narrower, connecting privacy to notions of autonomy and self-development:

> Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development. So understood, privacy is fundamentally dynamic. In a world characterized by pervasive social shaping of subjectivity, privacy fosters (partial) self-determination. It enables individuals both to maintain relational ties and to develop critical perspectives on the world around them.[40]

To Cohen, privacy is valuable, in part, because it permits self-development which is necessary for the development of the informed citizenry on which the viability of liberal democracy depends.[41] To achieve this end, society must protect the physical, economic, and mental safety of the marginalized,[42] all of which we would call forms of safety.

2. A Typology of Privacy

Others take a very different approach to defining privacy. In an original and thorough recent article, *A Typology of Privacy*, (hereinafter *Typology*) a group of scholars led by Bert-Jaap Koops offer a lens by which to rethink our understanding of privacy. These scholars identify eight basic, or "ideal," types of privacy, and a ninth type that overlaps with and touches each of them.[43] *Typology* claims that privacy "can be captured by [this] set of related concepts that together constitute privacy."[44] The eight ideal types are: (1) bodily, (2) spatial, (3) communicational, (4) proprietary or property-based, (5) intellectual, (6) decisional, (7) associational, and (8) behavioral.[45]

The overlay, which does not completely overlap with the eight ideal

39. Cohen, *supra* note 16, at 1906.

40. *Id.*

41. *Id.* at 1912–18.

42. *See id.*

43. Koops et al., *supra* note 13, at 566–68.

44. *Id.* at 488 (emphasis omitted).

45. *Id.* at 566–68.

types, is informational privacy.[46] Despite recognizing the frequency with which informational privacy is treated as a distinct type of privacy, the authors argue that, because "each ideal type of privacy contains an element of informational privacy," it is better understood as an overlay.[47]

As to the eight ideal types of privacy, the authors have analyzed their similarities and differences along certain "dimensions." They first map them along a spectrum of four zones of privacy, running from "the personal or completely private zone to intimate, semi-private, and public zones."[48] Building here on Alan Westin's foundational categorization of solitude, intimacy, anonymity and reserve,[49] as well as work by Roger Clarke, Anita Allen, Rachel L. Finn, David Wright and Michael Friedewald, the authors offer the following definitions:

> The intimate zone is characterized by a shift towards social engagement, albeit limited to intimate partners, family members, and close friends, as well as activities that take place in private and fenced-off spaces, such as the home where people share their life with intimate partners and family. The semi-private zone includes social interaction with a wider range of actors, including acquaintances, work colleagues, and professional relationships (e.g., interacting with a doctor, service provider or shop), and activities that occur in more quasi-public space. The public zone is typified by activities occurring in public—for example, in a public square, on public transportation, or on publicly accessible electronic platforms—where the privacy interest is characterized by the desire to be inconspicuous despite being physically or virtually visible in public space. This zone sits at the edge of the outer layer of privacy and social life.[50]

The authors also map their eight ideal types along the spectrum of negative and positive freedom, although they concede this distinction has some difficulties.[51] Finally, they map the types based on distinctions between "restricted access and subsequent control after access has been granted."[52] On this point, they note that, generally:

> This dimension is not independent from the other two, but rather combines both in the sense that restricted access is associated more (but not exclusively) with the private than with the public

46. *Id.* at 568.

47. *Id.* at 568–69.

48. *Id.* at 564.

49. *See supra* section I.A.1.

50. Koops et al., *supra* note 13, at 564 (emphasis omitted).

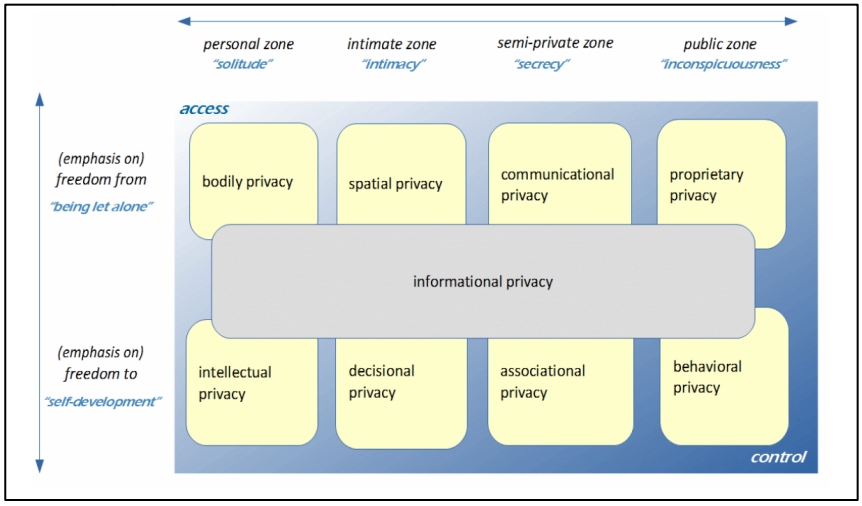
51. *Id.* at 565.

52. *Id.*

> zone, and more with negative freedom than with positive freedom, while control after access is more significant in the semi-private and public zones and has more the character of a positive freedom (self-determination) . . . . For example, any privacy interest in a person's behavior in public space has more to do with controlling the use of information about that activity than it does with restricting access (since some access has already been granted by the nature of the space itself). On the other hand, bodily privacy is typically (although not always) a question of access, rather than control.[53]

The authors also give us a graphical summary of the *Typology*'s landscape:

Figure 1:
Summary of the Privacy Typology[54]



Our overall conception of privacy is as broad as that in the *Typology*: it includes negative and positive freedom; it refers to restricted access and restricted post-acquisition use; it includes physical aspects of privacy as well as informational aspects. That said, our focus on safety means that we first emphasize directly physical privacy, and only then intellectual privacy, followed by economic and other forms of privacy, although informational privacy also remains important because the safety issues we discuss arise from allowing others to acquire information about

53. *Id.*

54. *Id.* at 484.

their target.

Claims to each of these aspects of privacy, whether or not they are claims to a "right" of privacy, include demands to be able to exclude others, or their mechanical proxies, from places and things, including, but—importantly—not limited to, data. Privacy protects access to physical bodies, and it protects against the observation of facts about the location and activities of bodies. It also does similar work for our things: inhibiting or preventing access to them, the observation of them, and the collection of information about their location, uses, and characteristics. Because our discussion involves so much of what the *Typology* deems the overlay of informational privacy, we turn to a brief discussion of informational privacy.

3. Informational Privacy

Persons can control the release of information about themselves in different ways, depending on the circumstances. Controlled access might be achieved, for example, by unobservability,[55] by untraceability,[56] by anonymity,[57] or by pseudonymity. This Article thus involves minimal discussion of the aspects of privacy that motivate much work on data protection, where the focus is frequently on limiting a recipient's use of another's data. Such legal limits, notably those in GDPR,[58] undoubtedly protect privacy in different and sometimes more general ways than the one that demands our attention here,[59] as those aspects of privacy fail to engage issues of safety as directly as the aspects we have chosen to focus on.

Admittedly, it is not difficult to formulate or even justify many "claims

---

55. "Unobservability is when you can not be observed. For example, shutting the door to the bathroom offers unobservability." Adam Shostack & Paul Syverson, *What Price Privacy? – and Why Identity Theft is About Neither Identity Nor Theft*, *in* ECONOMICS OF INFORMATION SECURITY 129, 130 (L. Jean Camp & Stephen Lewis, eds. 2004).

56. "Untraceability is when you cannot be traced from one identity to another. For example, 'John, who we play softball with, but don't know his last name' is untraceable; you can't track down a phone number for him." *Id.*; *see also* A. Michael Froomkin, *Anonymity and Its Enmities*, 1 J. ONLINE L. art. 4 (1995) [hereinafter, Froomkin, *Anonymity*], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715621 (last visited Mar. 9, 2020) (distinguishing between traceable and untraceable forms of anonymity and pseudonymity).

57. "Anonymity is when you are without any identifiers." Shostack & Syverson, *supra* note 55, at 130.

58. *See* GDPR, *supra* note 14.

59. "Informational self-determination is when you are confident that information you provide will be used only in ways you understand and approve. Giving your mother your new phone number probably qualifies." Shostack & Syverson, *supra* note 55, at 130.

to exclude" as claims to prevent others from learning facts about oneself, and thus to formulate claims to exclude as claims about data, broadly defined. That is, excluding people from one's home prevents others from seeing quite how horrible one is before one's morning coffee. Excluding people from one's credit-card records prevents them from seeing how cheap or spendthrift one may be. Excluding others from one's medical records protects against employment consequences, or just embarrassment, that might arise from one's health problems being publicized. Excluding the world from one's diary secures the freedom to experiment with stupid or potentially unpopular ideas.

It is important to note, however, that the privacy which prevents access to bodies and things, and to facts about bodies and things, is not simply regulating the management of data about persons—in most cases it forbids or even makes physically impossible the collection of those data. That can be a distinction with a difference.[60]

B. Safety

"Safety," like privacy, is a malleable concept. It is also potentially quite broad, and we mean to use it broadly. By "safety," we mean, first, the ability to protect one's bodily integrity, and that of one's family and associates, from physical harms and/or threats. Secondarily, we mean the ability to protect one's livelihood and one's possessions (and that of family and associates) from harm, or threat or diminishment. Both of these types of safety protect against an array of potential exercises of unjustified coercive power, ranging from threats of violence, to blackmail, to routine price discrimination. And as explained below, both of those types of safety can be indirectly secured or at least enhanced by the protection of privacy. Furthermore, to the extent that privacy can create a sense of safety and security, it may provide important psychological benefits, translating at times into physiological ones.[61]

We therefore adopt a definition of "safety" that may not be intuitively obvious. For example, we treat situations that may subject an individual to atypical economic coercion as dangers that may make one unsafe. Similarly, we treat blackmail—which threatens shame—as a safety threat. Arguably, the capability to impose substantial emotional stress is itself a

60. *Cf.* A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461 (2000) (arguing for regulation of data-collection technology in part because once data is collected it is harder to regulate); A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713 (2015) (proposing that some surveillance technology be regulated as environmental damage).

61. *See infra* text accompanying note 76 and sections III.B.1, B.2.

safety threat if only because emotional stress can have physical effects.

To argue that privacy (as defined) is safety (as defined), or at least can be a substantial contributor to safety, is (1) to argue that in many cases privacy reduces certain dangers and (2) to argue, implicitly or explicitly, that safety from those dangers is at least good and legitimate,[62] and perhaps even necessary for the enjoyment of some other right, e.g., rights to life, liberty, or property. The instrumental argument that privacy is safety engages implicitly or explicitly with claims (or counter-claims) that privacy is harmful, for instance, that it actually makes people less safe. These competing instrumental claims clash in the shadow not only of claims that privacy is itself a human right[63] (in which case claims that privacy is harmful might lose relevance), but also of claims that various other human rights are furthered by privacy or a lack thereof. Thus, for example, the twin debates over the legal regulation of cryptography and over legal demands for data-retention policies have largely consisted of factual assertions about how those policies will protect or harm individuals.[64] However, these debates have also at times touched on these policies' interactions with rights to freedom of expression, to freedom of association, and even to property.[65]

In Part III, below, we describe how a variety of existing legal rules reflect a recognition that privacy enhances safety. As regards our discussion of the dangers that privacy protects against, we adopt a worst-case-analysis framework in the interest of simplification. By focusing on the danger to the individual (harms that have some probability of happening), rather than on risk (which implies a measure of the actual likelihood of the event), we focus on the capabilities of those against whom privacy is interposed as a defense, rather than engaging with the intruder's intentions. By using the word "intruder," we mean to connote both an intrusion into someone's private affairs such as informational privacy breach and also an actual physical intrusion. The intentions of people, firms, and governments are not only varied but often opaque; a focus on capabilities rather than intentions reduces the scope of what remains a large and difficult problem, as one need not try to read minds. Similarly, we leave for another day a discussion of cost-benefit calculations, in which one tries to compare alleged costs of privacy with

62. This is so because, while privacy is sometimes assailed as a negative, safety is almost always viewed as a positive, although there can be exceptions: making terrorists safer is not, we presume, generally considered a positive.

63. *See infra* text accompanying notes 213 and 335.

64. *See infra* section III.E.3.

65. *See id.*

alleged benefits, as these too require an assessment of probable, rather than simply possible, actions.

II. THE ROLE OF SAFETY IN CONTEMPORARY PRIVACY THEORY

Contemporary privacy theory, by and large, pays too little attention to the ways in which privacy enhances safety. That does not mean that contemporary privacy theorists fail to recognize the point, just that few of them address it in any detail, perhaps because it seems obvious, or perhaps because the idea is not central to their arguments.

The failure to address privacy's impact on safety may also be a result of the specific approaches, discussed in section I.A.1 above, that scholars have taken in their attempts to describe privacy. One common approach to defining the term has been the attempt to "develop a unitary conception of privacy in the form of a unified conceptual core,"[66] which is most similar to how we generally define terms. To those taking this approach, safety is likely an afterthought.[67] Interrelated though we argue privacy and safety are, we do not suggest that safety forms the very core of privacy's meaning or value.

The second typical approach to defining privacy has been to catalogue different types or aspects of privacy and "mak[e] meaningful distinctions between" them.[68] This approach is obviously descriptive rather than prescriptive, but it can still offer hints at a definition of privacy by locating its common, and perhaps necessary or sufficient, characteristics or conditions. One might expect safety to figure more prominently under this approach, as there clearly exist clusters of privacy protections that bear on safety. Yet, with the partial exception of the *Typology*, which does discuss safety at times, we see little of this in the literature.

A third approach treats privacy as inherently good. This is the approach taken by authors like Julie Cohen. Other than to note that preserving the "breathing room" for the self is necessary for the self-development that enables both human flourishing and meaningful democratic participation,[69] Julie Cohen's work does not focus on the interplay of privacy and safety. To Cohen, privacy is not simply of instrumental value. It is inherently good. Pushing back against the commoditization of privacy, Cohen argues that privacy's rightful place is alongside values like

66. *See* Koops et al., *supra* note 13, at 487; Solove, *supra* note 12, at 1095–99.

67. *See supra* text accompanying note 15.

68. Koops et al., *supra* note 13, at 487; Solove, *supra* note 12, at 1095–99.

69. *See* Cohen, *supra* note 16, at 1906 and text accompanying notes 40–41.

dignity, equality, and freedom, because it is a necessary condition for the development of the self.[70] To Cohen, "the values of informational privacy are far more fundamental" than a mere matter of preference or taste.[71] "A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and serves vital individual and collective ends."[72]

A fourth approach is the one that most often leads scholars to expressly connect privacy to safety. It is a "reductionist approach[] that define[s] privacy as instrumental to realizing a more basic human value, such as liberty, autonomy, property, or bodily integrity."[73] In some ways, this instrumental approach is not about defining privacy but identifying its value. That makes it most likely to discuss safety. The relationship between privacy and safety grows less out of a definition of privacy than from an understanding of its practical value. Still, even where authors address the instrumental value of privacy, they often omit any mention of safety.[74]

The instrumental approach is, in a sense, the one adopted by this Article. Our definition of privacy is, as noted above, encompassing. On the other hand, we make no claim that safety enhancement is a necessary or sufficient condition for privacy. Instead, we argue that one way in which privacy is valuable is its ability to enhance safety. Whether it is necessary or sufficient for safety will vary with the circumstances.

---

70. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

71. *Id.* at 1423.

72. *Id.*

73. Koops et al., *supra* note 13, at 492; *see also, e.g.*, Judith J. Thompson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 272 (Ferdinand D. Schoeman, ed., 1984) (arguing that privacy, as a concept, is worthless because the term, as generally used, simply amounts to a group of other, more fundamental, interests).

74. *See, e.g.*, Solove, *supra* note 12, at 1093–94 (listing the fundamental interests instrumentally enhanced by privacy, neglecting to mention safety, and going on to state that "[s]ociety's commitment to privacy often entails restraining or even sacrificing interests of substantial importance, such as . . . efficient law enforcement"). Solove also references the portion of privacy discourse that views "the value of privacy in terms of furthering a number of different ends." *Id.* at 1145. In fact, this is Solove's approach: "I contend that privacy should be valued instrumentally." *Id.* at 1144. Looking to prior scholarship, Solove states, "Fried claims that privacy fosters love and friendship. Bloustein argues that privacy protects dignity and individuality. Boling and Inness claim that privacy is necessary for intimate human relationships. According to Gavison, privacy is essential for autonomy and freedom." *Id.* at 1145 (citations omitted). Then, looking to his own instrumental understanding of privacy, he notes that "there are a number of candidates for the value of privacy, as privacy fosters self-creation, independence, autonomy, creativity, imagination, counter-culture, freedom of thought, and reputation." *Id.* at 1145–46. Thus, we see that even in the scholarship that argues for an instrumental valuation of privacy, and lists the interests furthered by privacy protections, safety rarely if ever makes the list.

In any event, regardless of why privacy is generally not recognized as enhancing safety, our research suggests there is an absence that needs filling. Of contemporary works that do address the relationship, most do so only in passing,[75] although there are a few important exceptions.

A leading and significant exception to this near-rule is Alan Westin, who, in his seminal *Privacy and Freedom*, suggested that privacy has its deepest roots in the evolutionary drive towards safety. Nature, he claimed, resounds with "defiant cr[ies] for privacy, given within the borders of the animal's private territory to warn off possible intruders."[76]

For Westin, therefore, the desire for privacy arises fundamentally from a search for safety. Privacy promotes the physical safety of bodies and things by making it harder for would-be intruders to intrude.[77] It protects something in the nature of "economic safety" by "regulating density to available resources."[78] Protecting these resources is also arguably connected to physical safety insofar as scarcity threatens physical health. Westin also recognizes how overcrowding, i.e., a lack of personal space, leads to increased aggression and infighting within communities as members attempt to access scarce resources (and perhaps also as the result of a biological imperative to control crowding).[79] Finally, Westin notes that privacy promotes safety from illness, as a lack of space leads humans and animals to "high blood pressure, circulatory diseases, and heart disease."[80]

Turning then to humans, Westin quotes from Robert Merton's Social

---

75. Even in Koops et al., *supra* note 13, where the authors discuss several aspects of privacy that are related to safety, they do not consider it as a category. In discussing the types of privacy protected in the constitutions of various nations, the authors identify spatial privacy–the protection of the home and other places–which could enhance physical safety (by, perhaps, preventing police officers from storming in and initiating an armed confrontation) and mental safety or wellbeing. *See id.* at 515–16. They identify proprietary, or property-based, privacy, which could enhance economic safety. *See id.* at 516–18. They identify privacy of computers, which could enhance mental safety or wellbeing (by avoiding embarrassment, perhaps about one's browser history) and economic safety. *See id.* at 518–20. They identify the privacy of the person, part of which is the protection of the body of the person, which clearly could enhance physical safety and mental safety or wellbeing. *See id.* at 529–31. They expressly note, for example, that the Fourth Amendment to the United States Constitution protects the right of people to be "'secure in their persons'" against unreasonable search and seizure, which incorporates the inviolability of the body. *Id.* at 530. They even cite U.S. Supreme Court cases in which the Fourth Amendment operated to protect against physical intrusions into one's body. *Id.* at 530 n.170. Still, the ability of privacy to enhance safety is never discussed, in such terms, as one of the values of privacy.

76. WESTIN, *supra* note 21, at 9.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.* at 10 (internal citation omitted).

Theory and Social Structure in arguing that, without privacy, the average individual would descend into madness: individuals' "need" for privacy is the

> counterpart to the functional requirement of social structure that some measure of exemption from full observability be provided for. Otherwise, the pressure to live up to the details of all (and often conflicting) social norms would become literally unbearable; in a complex society, schizophrenic behavior would become the rule rather than the formidable exception it already is.[81]

Building on Westin's ideas, Adam D. Moore argues that privacy "is necessary for the species."[82] He cites a study finding that, when rats are placed in a quarter-acre pen without any privacy, their numbers never exceeded 200.[83] Even when the population reached 150, "fighting became so disruptive to normal maternal care that only a few of the young survived."[84] But when privacy protections were put in place, that same quarter-acre pen was able to support 5,000 rats.[85] Moore concludes, then, "that having the ability to separate, like food and water, is a necessity of life."[86]

Moore extends this conclusion to the human animal. He, like Westin, recognizes a "link between a lack of privacy and psychological and physical disorders in humans [as well as] nonhuman animals."[87] Modern studies on overcrowding in prisons support Moore's conclusion: the lack of personal space attendant to incarceration "has been linked to violence, depression, suicide, psychological disorders, and recidivism."[88] Moore then shifts his focus, arguing that "it is only through enhanced privacy protections that we can obtain appropriate levels of security against industrial espionage, unwarranted invasions into private domains, and information warfare or terrorism."[89] Relatedly, Moore recognizes that privacy promotes security in the context of encryption.[90]

---

81. *Id.* at 58 (quoting ROBERT MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 375 (1957)).
82. ADAM D. MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 48 (2010).
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.* at 55.
88. *Id.* at 55–56.
89. *Id.* at 207.
90. *Id.* at 208–09 ("Although the National Security Administration's position is that the widespread

A quite different, if equally rare, example of scholarship addressing the interaction of privacy and safety is Ruth Gavison's 1980 article *Privacy and the Limits of Law*.[91] Gavison recognizes the instrumental value of privacy, noting that one such benefit is "mental health."[92] Interestingly, though, she argues that the opposite can be true simultaneously—that privacy may be harmful to mental health.[93] Gavison is receptive to those "critics of contemporary society" who argue that "we suffer from too much privacy," that we deify the private sphere and ignore public aspects of life such that "individuals are alienated, lonely, and scared."[94]

To Gavison, then, privacy is a double-edged sword, especially when it comes to health and safety. In fact, despite her general view that privacy is good, she states:

> [t]here is something comforting and efficient about [a] total absence of privacy for all. A person could identify his enemies, anticipate dangers stemming from other people, and make sure he was not cheated or manipulated. Criminality would cease, for detection would be certain, frustration probable, and punishment sure. The world would be safer, and as a result, the time and resources now spent on trying to protect ourselves against human dangers and misrepresentations could be directed to other things.[95]

But although claiming that, with a "total absence of privacy," the "world would be safer," Gavison does concede that the subtraction of privacy would come at "much too high" a price.[96]

Similar to Gavison's recognition that privacy may, in some ways, be inimical to safety, Heidi R. Anderson argues against the recognition of privacy in public.[97] She notes potential negative consequences of Westin's

---

use of encryption software will allow criminals a sanctuary to exchange information necessary for the completion of illegal activities, . . . [n]ational security for government agencies, companies, and individuals actually *requires* strong encryption. Spies have admitted to 'tapping in' and collecting valuable information on U.S. companies–information that was then used to gain a competitive advantage. A report form the CSIS Task Force on Information Warfare and Security notes that 'cyber terrorists could overload phone lines . . . disrupt air traffic control . . . scramble software used by major financial institutions, hospitals, and other emergency services . . . or sabotage the New York Stock Exchange.' Related to information war, it would seem that national security requires strong encryption, multilevel firewalls, and automated detection of attacks.").

91. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

92. *Id.* at 442.

93. *Id.* at 440 n.63.

94. *Id.*

95. *Id.* at 443 (internal footnotes omitted) (emphasis added).

96. *Id.*

97. *See* Heidi R. Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy*

latter two (and perhaps latter three) stages of privacy—those in which the individual claims a right to privacy despite engagement with the public sphere. Generally, Anderson's position is that privacy is harmful to the public good where it would prevent exposure of truthful information.[98] Specifically, she argues against laws that forbid the recording of police officers, noting, for example, that a failure to shine a light on police brutality, might lead to more of it.[99]

Illustrating the complex interplay between privacy and safety, Anderson notes that law enforcement's argument against being recorded is also founded on claims of safety enhancement. While Anderson argues that police officers' activities must be public in order to promote accountability and public safety, police officers reply that only by keeping their activities private can they effectively protect public safety:

> [P]olice officers and their supporters argue that the threat of constant surveillance and later distribution via the Internet is an unfair invasion of privacy that prevents [officers] from adequately doing their job. For example, officers may hesitate to take necessary action out of concern that a partial and possibly inaccurate video recording of that action will lead to the officers' firing or to bad police work. This concern, in turn, threatens the officers' reputation and public safety as a whole.[100]

While her inquiry into the privacy-safety dynamic is thus quite specific, Anderson recognizes that privacy and safety are connected, and her discussion—like Gavison's—reminds that the issue is not always straightforward.

As with Anderson and Gavison, Solove too recognizes that privacy is at times opposed to safety. In *Conceptualizing Privacy*, he writes that

---

in Public, 7 ISJLP 543 (2012).

98. *Id.*

99. *Id.* at 547–49.

100. *Id.* at 547. In *Nothing to Hide*, Solove takes up in more detail the issue of privacy's struggle against national security. Typically a strong defender of privacy, Solove argues that the contest between security and privacy is "skewed . . . too much to the security side." *See* DANIEL J. SOLOVE, NOTHING TO HIDE, at vii (2011). We tend to agree with that conclusion, but we also tend to reject the frame that produced it. Solove describes the privacy-safety interplay as one where privacy gains commonly mean security losses. While Solove goes out of his way to disclaim the strongest form of this position—stating that while "[s]ecurity and privacy often clash, . . . there need not be a zero-sum tradeoff"—what he appears to mean is that security and privacy can coexist: that proper regulation of security programs can allow them to be effective without impinging too severely on privacy. *Id.* at 207. Thus, in Solove's view, "[t]here is a way to reconcile privacy and security: by placing security programs under oversight, limiting future uses of personal data, and ensuring that the programs are carried out in a balanced and controlled manner." *Id.* But the very idea of "reconciling" privacy and security implies that they are countervailing-rather than synergistic-ideals. *See id.* at 5,207.

"[s]ociety's commitment to privacy often entails restraining or even sacrificing interests of substantial importance, such as . . . efficient law enforcement."[101] In *A Taxonomy of Privacy*, Solove lists "security"—along with free speech and efficient consumer transactions—as an interest to be balanced against privacy.[102]

A more optimistic view of safety does appear elsewhere in Solove's work, as he has written about the ways in which privacy can enhance safety:

> Disclosure[[103]] can also threaten people's security. For example, many people have good reason to keep their addresses secret, including victims of stalking and domestic abuse attempting to hide from those that threaten them, police officers and prosecutors fearing retaliation by criminals, celebrities desiring to avoid harassment by paparazzi, and doctors who perform abortions desiring to protect their family's safety. People want to protect information that makes them vulnerable or that can be used by others to harm them physically, emotionally, financially, and reputationally. For example, in *Remsburg v. Docusearch, Inc.*, a deranged man was obsessed with Amy Lynn Boyer. He purchased Boyer's Social Security number and employment address from a database company called Docusearch. The man went to Boyer's workplace and murdered her. The court concluded that "threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[104]

Our point is thus not that Solove—or any other scholar—fails to see the connection between privacy and safety. Solove in fact lists some of the same safety benefits of privacy as we do below, noting that privacy can protect physical, emotional, financial, and reputational safety.[105] But in the context of a lengthy and careful analysis of privacy harms, there is very little express discussion of how the absence of privacy can put safety at risk or how strong privacy protections can enhance safety. We therefore

---

101. Solove, *supra* note 12, at 1093–94.

102. Solove, *supra* note 11, at 480.

103. Solove defines "disclosure"–a subset of the dissemination harm that he identifies as one of the four general types of privacy harm–as "the revelation of truthful information about a person that impacts the way others judge her character." *Id*. at 491. This is in contrast to "breach of confidentiality," which he defines as "breaking a promise to keep a person's information confidential," and "exposure," defined as "revealing another's nudity, grief, or bodily functions." *Id.*

104. *Id.* at 477, 532–33 (citing Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06, 1008 (N.H. 2003)) (internal footnote omitted).

105. *Id*. at 532–33.

seek to establish that the relationship between privacy and safety does not receive the attention it deserves, and that even when scholars focus on it, they sometimes see the relationship as containing substantial contradictions and conflicts.

As suggested above, for scholars who believe that privacy has inherent, non-instrumental value, there is little call to address the ways in which privacy might enhance safety. And we do not seek in any way to criticize that view. Rather, we invoke these examples to explain why it is that even the most thoughtful and careful analyses of privacy commonly fail to address its safety-enhancing aspects.[106] We suggest that discussions of the value of privacy will be enhanced by redressing this imbalance.

III. PRIVACY AS SAFETY IN PRACTICE

Privacy enhances safety in several broad and overlapping ways: (1) it makes one physically safer; (2) it provides psychological security; (3) it makes one economically safer (and protects from some forms of invidious discrimination); and (4) it makes the exercise of various political rights safer.[107]

Our goal in this Part is to persuade the reader not only that in many cases privacy enhances safety (and that its absence can be dangerous), but also that in many cases U.S. law already recognizes and protects privacy in order to protect the safety of individuals in a wide variety of circumstances.

Our somewhat eclectic examples cut across all of the *Typology*'s four zones of privacy. Even though we believe that our examples do not fit perfectly into the *Typology*, in what follows we refer to it often in order to order to connect (and sometimes contrast) our project to the *Typology*'s state-of-the-art categorizations.

A. Bodily and Locational Privacy

The freedom from bodily threats is the most fundamental and personal form of safety. Bodily privacy relates to an individual's interest in his or her own physical body. A person's ability to control bodily privacy is directly related to that person's ability to control interactions with their

106. See, for example, the works cited in note 15, *supra*, which identify privacy's core value as related to autonomy and self-development but do not engage substantially with the interplay of privacy and safety.

107. Arguably, by reducing stress caused by surveillance and other invasions of privacy, it also makes one safer from illness, but we do not explore that in this Article.

environment and with other people.[108] The key concerns include the ability to exclude unwanted physical contact and to restrict information about an individual's body.[109]

If Alice wishes to harm Bob, she must first find him. Locational privacy, also redundantly known as "geolocational privacy," is the ability to keep secret where one is.[110] Locational privacy is thus a strong protector against all sorts of real and potential dangers to physical safety, making it one of the most powerful types of freedom from harm. The most extreme example of the value of location data comes from the U.S. Air Force, which boasted that the day after a militant posted a selfie posing in front of a command post, the Air Force used the geolocation data embedded in the digital file to send out drones with missiles to destroy the entire complex.[111] The shoe was on the other foot when researchers revealed that cumulative data from Strava, a fitness app, could be used to create usage 'heat maps' that disclosed the location of U.S. military bases.[112] According to Nathan Ruser, the maps pointed to likely "US military forward operating bases in Afghanistan, Turkish military patrols in Syria, and a possible guard patrol in the Russian operating area of Syria."[113] To make matters worse, when the Strava app first attempted to allow users to mark sensitive spots as private, the result often was to make them stand out instead.[114] Other fitness apps have been shown to be similarly revealing.[115]

---

108. Koops et al, *supra* note 13, at 567.

109. *Id.* at 498, 567.

110. *See*, *e.g.*, Andrew J. Blumberg & Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever*, ELEC. FRONTIER FOUND. (Aug. 3, 2009), http://www.eff.org/wp/locational-privacy [https://perma.cc/4Q2Y-ARJV] (providing a definition of location privacy); *see generally* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567 (2012) (discussing hiding one's location in order to bypass or make ineffective attempts to partition the Internet geographically).

111. Walbert Castillo, *U.S. Bombs ISIS Using Social Media Intel*, CNN (June 5, 2015, 5:15 PM), https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [https://perma.cc/UQA5-UH2B].

112. Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, WIRED (Jan. 29, 2018), https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/ [https://perma.cc/T2HL-8FZ4].

113. *Id.*

114. Rob Pegoraro, *The Strava Social Exercise App Can Reveal Your Home Address*, YAHOO FIN. (Feb. 7, 2018), https://finance.yahoo.com/news/social-exercise-app-can-give-away-home-address-182247535.html [https://perma.cc/PM5C-2KH9].

115. *See, e.g.*, Maurits Martijn et al., *This Fitness App Lets Anyone Find Names and Addresses for Thousands of Soldiers and Secret Agents*, DE CORRESPONDENT, https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-addresses-for-thousands-of-soldiers-and-secret-

As these incidents demonstrate, locational privacy's value is that it allows one to regulate access to one's body and one's things.[116] The examples below present a variety of illustrations of this fundamental principle, although the dangers they protect against are not in the main as dramatic as a deadly drone strike.

Perhaps nowhere in law is the close link between privacy and physical safety more explicitly recognized and addressed than in the criminal justice system. As a system designed to identify, capture, convict, and incarcerate potentially dangerous people, the criminal-justice system requires the ability to safeguard both witnesses and members of the system itself from harms by suspects, defendants, convicts, and their associates. Depending on the nature of the perceived threat, the system achieves these goals by hiding personal information—and sometimes hiding people.

1. Hiding People: Witness Protection

Criminal trials in the United States are almost inevitably public. This can expose witnesses to personal risk. For obvious reasons, the defendant against whom the witness testifies may seek to intimidate the witness or make an example out of them to scare off other potential witnesses. Privacy—through, for example, witness-protection programs—is the shield for these witnesses, keeping them safe before, during, and after trial.[117]

Similarly, police safeguard the identity of confidential informants in order to protect them from retaliation.[118] This qualified privilege also exists when the informant assisted in an undercover transaction,[119] and despite various risks associated with the use of confidential informants.[120]

---

agents/260810880-cc840165 [https://perma.cc/CY46-4RVE] (describing how fitness app could be used to find locations, and often names and addresses, of soldiers and covert operatives).

116. In terms of the *Typology*, we would put this in both the Personal Zone and also in the Proprietary Zone.

117. *See generally* Raneta L. Mack, *The Federal Witness Protection Program Revisited and Compared: Reshaping an Old Weapon to Meet New Challenges in the Global Crime Fighting Effort*, 21 U. MIAMI INT'L & COMP. L. REV. 191 (2013); Nora V. Demleitner, *Witness Protection in Criminal Cases: Anonymity, Disguise or Other Options*, 46 AM. J. COMP. L. 641, 641 (1998) (noting the conflict between ensuring witnesses' privacy and the U.S. Constitution's Confrontation Clause).

118. 21 AM. JUR. 2D CRIMINAL LAW § 1152 (2019) ("The prosecution in a criminal case is generally allowed to withhold from an accused the identity of an informer."); California v. Ortiz, No. B158369, 2004 WL 2251202, at *7 (Cal. Ct. App. Oct. 7, 2004) ("The confidential informant's anonymity is essential to his safety and well-being.").

119. 21 AM. JUR. 2D CRIMINAL LAW § 1152.

120. *See, e.g.*, ABA STANDARD FOR CRIM. JUST. Standard 2.4 (noting various risks that prosecutors

2. Hiding Information About People

a. In Criminal Justice

A broad form of privacy protection commonly applies to officials involved in law enforcement and the judiciary. The State of Florida, for example, has the broadest open-records policies in the United States[121]: as the Florida Supreme Court has noted, "[a]ll governmental entities in Florida are subject to the requirements of the Sunshine Law unless specifically exempted[,]"[122] making Florida the "Sunshine State" in more ways than one. But even Florida has long made an exception to this right of public access, protecting certain particularly sensitive personal information, such as the home addresses of officials in law enforcement, the judiciary, and other public positions whose occupants might draw the ire of an angry and vengeful citizen.[123]

Courts also recognize the importance of privacy for the safety of jurors in certain criminal cases. As part of the public's right to see justice done, and of the right of the defendant to a public trial, courts ordinarily make the jurors' identities public during or at the conclusion of a trial.[124] In

---

should consider before relying on testimony of confidential informant).

121. Sandra F. Chance & Christina Locke, *The Government-in-the-Sunshine Law Then and Now: A Model for Implementing New Technologies Consistent with Florida's Position as a Leader in Open Government*, 35 FLA. ST. U. L. REV. 245, 245 (2008).

122. Sarasota Citizens v. City of Sarasota, 48 So. 3d 755, 762 (Fla. 2010).

123. Florida law exempts from disclosure public records pertaining to the "home addresses, telephone numbers, dates of birth, and photographs of active or former sworn law enforcement personnel or of active or former civilian personnel employed by a law enforcement agency" FLA. STAT. ANN. § 119.071(4)(d)2.a (West 2019). The particular groups covered by the exemption are listed in the statute. *See id.* §§ (4)(d)2.c, l, m, r, t (providing similar protections (sometimes also including the place of employment) for other investigatory officials); *id.* § (4)(d)2.d (firefighters); *id.* §§ (4)(d)2.e, g, m (current and former justices of the Florida Supreme Court, (minus the bar on photographs, but also protecting the "places of employment of the spouses and children of current or former justices and judges; and the names and locations of schools and day care facilities attended by the children of current or former justices and judges") magistrates, judges, administrative law judges, child-support hearing officers, and other adjudicators); *id.* §§ (4)(d)2.f, l (current or former state prosecutors and public defenders); *id.* §§ (4)(d)2.h–k, o (state and local personnel managers, code enforcers, guardians ad litem, probation officers and other workers in the prison system); *id.* § (4)(d)2.q (EMTs and paramedics); *id.* § (4)(d)2.s (employees of addiction treatment facilities).

124. Although practice varies, in most jurisdictions the identities of the jurors, which can be found in the court record, are presumed to be public. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1145 (2002). Thus, circumstances in which the jurors are impaneled anonymously or the nature of the matter leads the court to seal the records of the case are exceptions to general practice; *see also* Kevin Delaney, *The Right of Access to Juror Names and Addresses*, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS (Summer 2016), https://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-summer-2016/right-access-juror-names-an [https://perma.cc/74BA-8QC7]; *see also, e.g.*, United

certain cases, however, courts keep the jurors' personal information private in order to prevent jury tampering or reprisals.[125] In other words, when necessary even strongly guarded principle of transparency of the trial process will bow to the safety needs of jurors and their privacy maintained even after the trial is over.

b. Protection from Abusers

The direct connection between locational privacy and physical safety is particularly clear in the context of domestic abuse and rape. There is a substantial body of scholarship demonstrating that when victims of stalking or domestic abuse regain control over their personal information—i.e., control over their informational and especially locational privacy—it protects their physical safety.[126] "[B]attered women are at elevated risk of violence during the pendency of prosecution,"[127] leading reformers to suggest that police, prosecutors, and courts should help victims avoid being found by their abusers.[128] On the other hand, it should also be noted that there is an important strand of scholarship that traced the law's unwillingness to interfere in marital battering to a belief that this would intrude into the privacy of the home.[129]

In fact, the Supreme Court has expressly recognized that privacy

---

States v. Wecht, 537 F.3d 222 (3d Cir. 2008); United States v. Doherty, 675 F. Supp. 719 (D. Mass. 1987); Commonwealth v. Long, 922 A.2d 892, 905 (Pa. 2007) (holding that there is a qualified First Amendment right of access to juror names but not addresses); State *ex rel*. Beacon J. Publ'g Co. v. Bond, 781 N.E.2d 180 (Ohio 2002).

125. *See* United States v. Blagojevich, 612 F.3d 558, 561 (7th Cir. 2010) ("Anonymous juries are permissible when the jurors' safety would be jeopardized by public knowledge, or the defendant has attempted to bribe or intimidate witnesses or jurors."); United States v. Eufrasio, 935 F.2d 553, 574 (3d Cir. 1991) ("A trial court has discretion to permit an anonymous jury without holding an evidentiary hearing on juror safety, if the court believes there is potential for juror apprehension."); Michigan v. Williams, 616 N.W.2d 710, 714 (Mich. Ct. App. 2000) (stating that anonymous juries should be used where "jurors' safety" is an issue).

126. *See, e.g.*, Paul S. Haberman, *Before Death, We Must Part: Relocation and Protection for Domestic Violence Victims in Volatile Divorce and Custody Situations*, 43 FAM. CT. REV. 149, 159 (2005) (proposing a model for relocation of abused spouses based upon the Federal Witness Protection Program).

127. Barbara Hart, *Battered Women and the Criminal Justice System*, 36 AM. BEHAV. SCIENTIST 625, 631 (1993) (proposing that the criminal justice system help victims prevent abusers from locating them).

128. *See, e.g.*, Kimberly D. Bailey, *It's Complicated: Privacy and Domestic Violence*, 49 AM. CRIM. L. REV. 1777, 1813 (2012) (stating that privacy can provide domestic violence victims with more choices and "more of a voice about which solutions are appropriate for their particular situation").

129. *See* JEANNIE SUK, AT HOME IN THE LAW: HOW THE DOMESTIC VIOLENCE REVOLUTION IS TRANSFORMING PRIVACY (2009).

protects physical safety in this context, noting that publishing the names of rape victims may jeopardize their "physical safety," as victims "may be targeted for retaliation if their names become known to their assailants."[130]

c. Protection from Kidnappers

Knowing where your target can be found is of obvious importance to potential kidnappers; the absence of locational privacy is what makes kidnapping possible. Kidnapping for profit is a major criminal market, with an estimated total turnover of up to U.S. $1.5 billion per year.[131] According to Gardaworld, a kidnap for ransom and maritime piracy risk mitigation service, most of the world is rated as "substantial," "severe," or "critical" risk for kidnapping or piracy, including Mexico and much of South America, most of Africa, India, China, and the former Soviet Union.[132] Non-terrorist kidnappers for ransom target "foreign tourists, high-net-worth local residents insured by multinational insurers, and the employees of foreign enterprises,"[133] but also domestic middle-class persons thought to have assets, and in Mexico even working-class individuals.[134] The process is almost institutionalized, to the point where "in many established kidnap hotspots, ransoms are indeed surprisingly low and stable."[135]

In order to prevent kidnappers from deducing their locations, potential targets need to avoid being tracked, and need to avoid predictable patterns of movement such as taking the same route home every day. Locational

130. The Florida Star v. B.J.F., 491 U.S. 524, 537 (1989); *see also* Kimberly W. Bacon, *Florida Sun v. B.J.F.: The Right of Privacy Collides with the First Amendment*, 76 IOWA L. REV. 139, 154 n.117 (1990).

131. Anja Shortland, *Governing Kidnap for Ransom: Lloyd's as a "Private Regime"*, 30 GOVERNANCE 283, 284 (2017).

132. *Kidnap and Piracy Threat Forecast Map 2019*, GARDAWORLD, https://www.garda.com/kidnap-and-piracy-threat-forecast-map-2019 [https://perma.cc/EG2B-C9J9].

133. Shortland, *supra* note 131, at 284.

134. Sergio Ramos, *Kidnapping Statistics in Mexico as of Feb 2014*, HAVOSCOPE (Apr. 11, 2014), https://web.archive.org/web/20140807051843/http://www.havocscope.com/kidnapping-statistics-in-mexico-as-of-feb-2014/ [https://perma.cc/QN9M-QXE3] (reporting that "69 percent of the victims were also considered to be non-affluent [including] . . . . middle class workers, shop owners students and mid-level professionals"); Ken Ellingwood, *Fear of Kidnapping Grips Mexico*, LA TIMES (Sept. 1, 2008), http://www.latimes.com/world/la-fg-kidnap1-2008sep01-story.html [https://perma.cc/9YMX-V82E] (reporting that half of kidnapping victims were middle-class and that "[t]here have been cases in which working-class families were ordered to pay as little as $500 to get a relative back").

135. Shortland, *supra* note 131, at 285.

information is, however, a double-edged sword in kidnapping prevention: persons who fear they or their relatives may be targets may want all family members to carry wearable GPS devices so that rescuers can find them if they are snatched.[136] This illustrates the fact that privacy need not be absolute to protect safety; rather, what matters is that a person be able to control who has access to information about themselves: in this case, where they are.

d. Protection from Stalkers

Similar issues arise when targets seek to avoid a stalker who is not seeking a kidnap, but rather seeks access (e.g., to a celebrity) or seeks intimidation or violence. The Internet often makes it easy for stalkers (and kidnappers) to obtain personal information about their potential victims.[137] This can facilitate, or even cause, online or in-person stalking—and worse.[138]

The Center for Disease Control reported, in 2010, that one in three women and one in four men had been victims of physical violence or stalking by an intimate partner.[139] Furthermore, one in six women and 5.2% of men in the United States reported experiencing "stalking victimization at some point during their lifetime in which they felt very fearful or believed that they or someone close to them would be harmed or killed."[140] An earlier study stated that about one quarter of stalking victims reported some form of cyberstalking also, such as email or texting.[141]

---

136. Santiago Montenegro, *Falling Kidnapping Rates and the Expansion of Mobile Phones in Colombia*, at 26 (Universidad de los Andes, Paper No. 12, 2009) (ISSN 1657-5334), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1544475 [https://perma.cc/7NHC-BL5U] (attributing fall in kidnappings to ability of victims to phone for help or be traced via cellphone); COGNIZANT, KIDNAP AND RANSOM INSURANCE: AT AN INFLECTION POINT 10 (Oct. 2015), https://www.cognizant.com/whitepapers/Kidnap-and-Ransom-Insurance-At-an-Inflection-Point-codex1575.pdf [https://perma.cc/EB4R-8J9U] (noting use of wearables as means of foiling kidnappings).

137. Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser & Sarah Tucker, *Intimate Partner Violence, Technology, and Stalking*, 13 VIOLENCE AGAINST WOMEN 842, 849 (Aug. 2007), https://doi.org/10.1177/1077801207302045 (noting that "[s]talkers are using . . . publicly available free Web sites and paid information brokers to obtain personal information").

138. Re "worse," see *infra* section III.A.2.e.

139. NAT'L CTR. FOR INJURY PREVENTION & CONTROL, CTR. FOR DISEASE CONTROL, NATIONAL INTIMATE PARTNER AND SEXUAL VIOLENCE SURVEY: 2010 SUMMARY REPORT 2 (Nov. 2011).

140. *Id.*

141. U.S. DEP'T OF JUST., BUREAU OF JUSTICE STATISTICS, NCJ 224527, STALKING VICTIMIZATION IN THE UNITED STATES (Jan. 2009), https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf [https://perma.cc/P3JS-RXN8].

Stalking can be combined with hacking personal devices or social media accounts in order to obtain, and sometimes publicize, personal data or intimate photos.[142] New technology also facilitates stalking in a more direct but no less disturbing manner. In an Australian case an ex-boyfriend "allegedly weaponized simple technology and smartphone apps that allowed him to remotely stop and start her car, control the vehicle's windows and track her constantly."[143] Next up, instead of having to follow in person, stalkers will use drones to follow their victims and photograph their every move.[144]

e. Protection from Doxing and Swatting

"Doxing" (or "doxxing"[145]) is the malicious acquisition and publication of non-public personal data about a target in the hopes that others will then use the information to harass or injure the target.[146] This can have tragic results. In 1997, an anti-abortion activist named Neal Horsely published the so-called "Nuremberg Files": a website listing names of approximately 200 abortion providers.[147] The site listed the providers' home addresses, phone numbers, and posted photos of them.[148] In an unsubtle encouragement to violence, the website noted which providers were still working, which had been wounded, and which had been killed.[149] Between 1993 and 2015, at least eight abortion providers were

142. Barbara McDonald, *Privacy, Princesses, and Paparazzi*, 50 N.Y. L. SCH. L. REV. 205, 235 (2005) ("[T]he publication of photographs, often taken in secret and while following a person continuously, either visibly or surreptitiously, add greatly to the subject's feelings of intrusion.").

143. Reis Thebault, *A Woman's Stalker Used an App that Allowed Him to Stop, Start and Track Her Car*, WASH. POST (Nov. 6, 2019, 8:40 PM), https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/ [https://perma.cc/FQC5-CQ37].

144. *See* A. Michael Froomkin & Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 CONN. L. REV. 1, 33 (2015) (suggesting that following someone with a drone could violate anti-stalking laws or be a civil nuisance); Kristen M.J. Thomasen, *Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation*, 16 CAN. J.L. & TECH. 307, 323 (2018).

145. Victoria McIntyre, *"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent*, 19 TUL. J. TECH. & INTELL. PROP. 111, n.5 (2016) ("Doxing is sometimes referred to as doxxing.").

146. *Id.* at 113.

147. David S. Cohen & Krysten Connon, *Strikethrough (Fatality): The Origins of Online Stalking of Abortion Providers*, SLATE (May 21, 2015, 3:38 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2015/05/neal_horsley_of_nuremberg_files_died_true_threats_case_reconsidered_by_supreme.html [https://perma.cc/N5K7-X7R4].

148. *Id.*; *see also* Hatewatch, *Anti-Abortion Extremist Neal Horsely Has Died*, S. POVERTY L. CTR. (May 11, 2015), https://www.splcenter.org/hatewatch/2015/05/11/anti-abortion-extremist-neal-horsley-has-died [https://perma.cc/KR47-D9NR].

149. Hatewatch, *supra* note 148; *see also* Horsley v. Feldt, 304 F.3d 1125, 1129 (11th Cir. 2002)

murdered by anti-abortion activists.[150]

The harassment that follows doxing can be intense. After the 2013 Boston Marathon bombing, individuals posting on Reddit and Twitter misidentified a number of suspects and published their personal information, including pictures, online.[151] One falsely identified person—a twenty-two-year-old named Sunil Tripathi—became the target of harassment and soon committed suicide.[152]

In a particularly powerful example, the New York Times reported in 2018 on the virtual disappearance of Dr. Christopher Filardi, an ornithologist who, in 2015, became the target of an Internet mob after his employer, the American Museum of Natural History, posted a photo of a rare male forest kingfisher that he had trapped in a net while doing zoological research in Guadalcanal.[153] Word then got out that Dr. Filardi had not just photographed the bird, but had killed it for the museum, where he then served as the director of Pacific Programs.[154] While Dr. Filardi worked in the field without Internet access, back home the Internet response, led by animal-rights activists, was savage vilification.[155] As matters snowballed, hackers attempted to access Dr. Filardi's Facebook account, which he then shut down; people also targeted his children's accounts. Nighttime callers phoned death threats to his wife and 3,798 people signed an online petition stating that "Chris Filardi is a disgrace

---

(noting that "on October 24, [1998], Horsley altered the Nuremberg Files website to graphically reflect which abortion providers had been wounded or killed; he did so by 'graying-out' the wounded and 'striking-through' the dead").

150. *See* Tara Murtha, *How Abortion Providers are 'Living in the Crosshairs'*, ROLLING STONE (May 18, 2015, 4:03 PM), https://www.rollingstone.com/politics/politics-news/how-abortion-providers-are-living-in-the-crosshairs-34307/ [https://perma.cc/M9KP-79FY]. A 2015 New York Times article found that "[a]t least 11 people have been killed in attacks on abortion clinics in the United States since 1993," but that number includes not just doctors, but also receptionists and a security guard, among others. *See* Liam Stack, *A Brief History of Deadly Attacks on Abortion Providers*, N.Y. TIMES (Nov. 29, 2015), https://www.nytimes.com/interactive/2015/11/29/us/30abortion-clinic-violence.html (last visited Mar. 9, 2020).

151. Dave Lee, *Boston Bombing: How Internet Detectives Got It Very Wrong*, BBC (Apr. 19, 2013), https://www.bbc.com/news/technology-22214511 [https://perma.cc/WQ5C-2GYA].

152. Traci G. Lee, *The Real Story of Sunil Tripathi, the Boston Bomber Who Wasn't*, NBC NEWS (June 22, 2015), https://www.nbcnews.com/news/asian-america/wrongly-accused-boston-bombing-sunil-tripathys-story-now-being-told-n373141 [https://perma.cc/434E-CB42]; *see also* Nellie Bowles, *How 'Doxxing' Became a Mainstream Tool in the Culture Wars*, N.Y. TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html (last visited Mar. 9, 2020).

153. Kirk W. Johnson, *The Ornithologist the Internet Called a Murderer*, N.Y. TIMES (June 15, 2018), https://www.nytimes.com/2018/06/15/opinion/sunday/moustached-kingfisher-internet-harassment.html (last visited Mar. 9, 2020).

154. *Id.*

155. *Id.*

and frankly does not deserve to breathe another breath."[156] When Dr. Filardi returned to work in New York, the police advised him to sneak in via a back door. When he published an essay defending his work, commentators called him a murderer.[157] Eventually, Dr. Filardi changed his job, scrubbed his online profile, and made himself hard to find.[158]

Most members of online mobs live far from their targets and thus they limit themselves to verbal abuse. Unfortunately, publication of personal locational information—whether self-published or the product of doxing—can lead to "swatting." This occurs when someone calls the police and falsely reports that a hostage situation or other scenario calling for a SWAT team—i.e., heavily armed police—is taking place at the target's home. The police then raid the home, an event that puts the unsuspecting inhabitants at risk.[159] In one case, the Wichita Police SWAT team responded to a call reporting a hostage-taking and—in circumstances that remain opaque—shot and killed the target.[160] While swatting commonly arises from private vendettas, victims include a prominent security researcher who angered an online doxer[161] and, more recently, three separate events targeted survivors of the Marjory Stoneman Douglas high-school shooting, who had each become nationally recognized gun-control activists.[162]

---

156. *Id.*

157. *Id.*

158. *See id.* (describing the effort required to contact Dr. Filardi).

159. *Swatting*, LEXICO OXFORD DICTIONARY, https://en.oxforddictionaries.com/definition/swatting [https://perma.cc/S929-XLUM] ("Swatting" is defined as "[t]he action or practice of making a hoax call to the emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address.").

160. Emanuella Grinberg, *Shooting Death in Video Game Leads to a Real One in Kansas*, CNN (Jan. 30, 2018, 7:24 PM), https://www.cnn.com/2018/01/30/us/kansas-swatting-death-affidavit/index.html [https://perma.cc/7CZT-W9D5].

161. *See* Brian Krebs, *The World Has No Room for Cowards*, KREBSONSECURITY (Mar. 13, 2013, 3:15 PM), https://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/ [https://perma.cc/6EUG-GPBN] (describing a SWATing incident at his home); Brian Krebs, *SWATing Incidents Tied to ID Theft?*, KREBSONSECURITY (Apr. 13, 2013, 4:47 PM), https://krebsonsecurity.com/2013/04/swatting-incidents-tied-to-id-theft-sites/ [https://perma.cc/YVS6-D29G] (describing research identifying possible culprit); Brian Krebs, *Serial Swatter, Stalker and Doxer Mir Islam Gets Just 1 Year in Jail*, KREBSONSECURITY (July 16, 2016, 8:32 PM), https://krebsonsecurity.com/2016/07/serial-swatter-stalker-and-doxer-mir-islam-gets-just-1-year-in-jail/ [https://perma.cc/728Z-2X3P] (reporting on trial of person partly responsible for SWATing Krebs).

162. Erika Pesantes, *Swatting Hoax Targets #NeverAgain Activists*, SUN SENTINEL (June 8, 2018, 9:45 AM), http://www.sun-sentinel.com/local/broward/parkland/florida-school-shooting/fl-sb-swatting-hogg-kasky-20180608-story.html [https://perma.cc/C8MH-PXJM] (reporting swatting attack on David Hogg and Cameron Kasky, and noting the presence of family members in Kasky's home); Jeff Tavss & Alex Finnie, *Family of Stoneman Douglas Student Advocate David Hogg 'Swatted' at Home*, ABC NEWS 10 (June 5, 2018, 6:13 PM), https://web.archive.org/web/20190331

Most recently, parents of children who survived the December 2012 Sandy Hook elementary-school massacre issued an open letter describing the attacks they suffered after the tragedy:

> Conspiracy groups and anti-government provocateurs began making claims on Facebook that the massacre was a hoax, that the murdered were so-called "crisis actors" and that their audience should rise up to "find out the truth" about our families. These claims and calls to action spread across Facebook like wildfire and, despite our pleas, were protected by Facebook.
>
> . . . .
>
> We have endured online, telephone, and in-person harassment, abuse, and death threats. In fact, one of the abusers was sentenced to jail for credible death threats that she admitted in court she had uttered because she believed in online content created by these "fringe groups". [Sic] In order to protect ourselves and our surviving children, we have had to relocate numerous times. These groups use social media, including Facebook, to "hunt" us, posting our home address and videos of our house online. We are currently living in hiding.[163]

When telephone books were the main means for ordinary people to find out where others lived, anyone wishing to could ask the telephone company to keep them out of the book by paying a small fee for an unpublished or even unlisted (not available via directory assistance) number.[164] Between the Internet and modern consumer data bases, hiding one's home address nowadays has become nearly impossible. As a result, anyone who has the misfortune to become an involuntary public figure is at risk.[165]

133339/https://www.local10.com/news/parkland-school-shooting/family-of-stoneman-douglas-advocate-david-hogg-swatted-at-home [https://perma.cc/5UPB-QP7A] (noting there were no casualties in the David Hogg incident as the house was empty at the time); Sharon Aron Baron, *Police Respond to Threat Against Parkland Activist and Bomb Scare at Walmart*, CORAL SPRINGS TALK (June 11, 2018), http://coralspringstalk.com/police-respond-to-threat-against-19571-19571 [https://perma.cc/86DJ-SCPK] (reporting swatting incident targeting Sarah Chadwick).

163. Leonard Pozner & Veronique De La Rosa, *An Open Letter to Mark Zuckerberg: Our Child Died at Sandy Hook – Why Let Facebook Lies Hurt Us Even More?*, THE GUARDIAN (July 25, 2018, 6:00 AM), https://www.theguardian.com/commentisfree/2018/jul/25/mark-zuckerberg-facebook-sandy-hook-parents-open-letter [https://perma.cc/27LH-CQ5J].

164. *See* Peter F. Kriete, *Caller ID and the Great Privacy Debate: Whose Phone Call is it, Anyway?*, 97 DICK. L. REV. 357, 366 (1993).

165. For example, after U.C. Berkeley law professor John Yoo appeared on a Fox News show and accused Lt. Col. Alexander Vindman of "espionage," Vindman's lawyer alleged that "LTC Vindman and his family have been forced to examine options, including potentially moving onto a military base, in order to ensure their physical security in the face of threats rooted in the falsehood that Fox News originated." Letter from David Pressman, Bois Schiller Flexner LLP, to Lily Fu Claffee,

f. Protection of Beneficiaries of Good Fortune (Lottery Winners)

Good fortune can also be a source of both physical and economic danger. The downside of good fortune emerges most starkly in the case of winners of large lottery payments. While winning the lottery may seem to be an occasion for celebration, it can also be the source of harassment and pain.[166] State lotteries historically required that winners of large prizes agree to have their names and often photos publicized.[167] The policy serves the twin goals of publicity for the lottery and transparency as to who is winning—the latter being designed to make it more difficult for insiders to manipulate the lottery results. In a break with this trend, several states now allow winners to be anonymous, or allow a period of anonymity,[168] thus allowing winners to prepare for the tsunami of what a New Hampshire court called "solicitation and harassment."[169]

Executive VP and General Counsel of Fox News, at 2–3 (Nov. 20, 2019), https://www.documentcloud.org/documents/6555531-VIndman-Boies-LETTER.html [https://perma.cc/9ZP3-FACA]. The U.S. Army issued a statement that it was providing "security assistance" to Lieutenant Colonel Alexander Vindman in order "to ensure that he and his family are properly protected." Luis Martinez, *Army Providing Security Assistance to Vindman, a Key Witness in Impeachment Hearings*, ABC NEWS (Nov. 19, 2019, 11:51 AM), https://abcnews.go.com/Politics/army-providing-security-assistance-vindman-keywitnessimpeachment/story?id=67137282 [https://perma.cc/YTW4-NPH9].

166. *See* Jen Doll, *A Treasury of Terribly Sad Stories of Lotto Winners*, THE ATLANTIC (Mar. 30, 2012), https://www.theatlantic.com/national/archive/2012/03/terribly-sad-true-stories-lotto-winners/329903/ [https://perma.cc/4R92-5Q2A].

167. *See* Frank D. LoMonte, *Who's Willing to Bet That State Lotteries are Free of Manipulation?*, WASH. POST (June 12, 2018, 3:05 PM), https://www.washingtonpost.com/opinions/whos-willing-to-bet-that-state-lotteries-are-free-of-manipulation/2018/06/12/f9832e50-6dc0-11e8-afd5-778aca903bbe_story.html (last visited Mar. 9, 2020). Of the states permitting some form of anonymity listed *infra* note 168, Kansas was the first to permit winners to remain anonymous. *See* KAN. STAT. ANN. § 74-8720 (2019); *see also* Kan. Sess. Laws ch. 246 (1991) (requiring no disclosure of winner's identity without written permission).

168. David Pitt, Associated Press, *Should Lottery Winners' Names be Secret? States Debate Issue*, BUS. INSIDER (Jan. 15, 2016), https://www.businessinsider.com/ap-should-lottery-winners-names-be-secret-states-debate-issue-2016-1 [https://perma.cc/DPL4-NWKX] ("Delaware, Kansas, Maryland, North Dakota, Ohio and South Carolina allow winners to remain anonymous. A growing number of other states, including Colorado, Connecticut, Massachusetts and Vermont, will award prizes to a trust and allow a trustee–usually an attorney–to collect without disclosing the name of the ticket holder. States including Illinois and Oregon have made exceptions to their policy of disclosure when winners demonstrate a high risk of harm."). More recently, Mississippi, North Carolina, and West Virginia have passed similar laws. *See* Mississippi, MISS. CODE ANN. § 27-115-43 (2018); 2018 Miss. Laws 1st Ex. Sess. ch. 2 § 22 (no disclosure without written permission), North Carolina, N.C. GEN. STAT. ANN. § 18C-132 (2019) (winners of over $50 million may remain confidential for 90 days upon request); *see also* 2019 N.C. Sess. Laws 142 § 5; West Virginia, W. VA. CODE § 29-22-15a (2018); 2018 W. Va. Acts 884.

169. Jane Doe v. New Hampshire Lottery Comm'n, No. 226-2018-CV-00036, at 5–6 (Hillsborough Sup. Ct. S.D.N.H. Mar. 12, 2018), https://www.courts.state.nh.us/caseinfo/pdf/civi

Harms to lottery winners are surprisingly common. Lottery winners have, on several occasions, suffered from violence and extortion. In one case, a winner's brother hired a hit man to kill him.[170] In another case, a Florida man vanished three years after winning $31 million, only to be found under a concrete slab a few years later.[171] One pair of Irish lottery winners went into hiding to escape extortion by an armed gang.[172] With some regularity, winners are targets for theft and fraud.[173] Even when there is no violence, winners face multiple demands for money from friends, relatives, and strangers; others, surprisingly, face various forms of contempt or mockery.[174]

B. Intellectual Privacy

Intellectual privacy comprises a person's interest in the privacy of his or her personal thoughts, opinions, and beliefs. Protecting intellectual privacy ensures that one is free to be oneself—at least in one's own mind.[175] Whereas bodily privacy is concerned with the physical aspect of the individual, intellectual privacy is concerned with the mental, emotional, or spiritual aspects of the individual.[176] Intellectual privacy is less tangible than some other privacy rights, and thus often is seen in conjunction with those other rights, like associational and decisional privacies.[177] Although difficult to enforce as an independent right, the freedom to believe and think whatever a person wishes is fundamental to and a necessary condition of many of the other extant privacy rights. For example, there is a close connection between intellectual privacy and the freedom to express one's beliefs or thoughts, which in turn has large implications for political freedom.

---

l/DoevNHLC/031218doevNHLC.pdf [https://perma.cc/AWW3-BJSG].

170. Doll, *supra* note 166.

171. *Abraham Shakespeare Won the Lottery, Then Lost it All*, TAMPA BAY TIMES (Jan. 24, 2009), https://www.tampabay.com/news/From-the-archives-Abraham-Shakespeare-won-the-lottery-then-lost-it-all_164452713/ [https://perma.cc/W728-WD7W].

172. Alan Murdoch, *Lottery Winners Forced to Go Into Hiding After Extortion Attempts*, THE INDEPENDENT (Apr. 16, 1994, 12:02 AM), http://www.independent.co.uk/news/uk/lottery-winners-forced-to-go-into-hiding-after-extortion-attempts-1370272.html [https://perma.cc/H5VT-CCB7].

173. *Id.*

174. Doll, *supra* note 166 (describing "ugly" comments aimed at one winner by "lotto snobs" and at another winner for being supposedly too old to enjoy the winnings).

175. NEIL RICHARDS, INTELLECTUAL PRIVACY (2015); Koops et al., *supra* note 13, at 567.

176. *Id.*

177. *Id.* at 555.

1. Protection of Psychological Safety

In addition to its value to physical safety, privacy—particularly intellectual privacy—helps create a zone of psychological safety. However, as with physical safety, the relationship between privacy and psychological wellbeing can be somewhat double-edged: too much privacy can become negative isolation and enforced privacy can be the product of ostracism or solitary confinement. Indeed, privacy only means something in relation to others—privacy was not a concern for Robinson Crusoe, but rather the opposite. While aware of these caveats, here we concentrate on the positive side of the relationship.

There is now extensive evidence regarding the psychological costs of feeling threatened. For example, the stress of being stalked "can lead to severe depression, helplessness, and mental dysfunction."[178] In *Winston v. Lee*,[179] the U.S. Supreme Court recognized what may seem obvious to many: that privacy contributes to making people feel safer from physical harm.[180] The Court noted that intrusions such as the police entering a person's living room,[181] eavesdropping on someone's telephone calls,[182] or forcing a person to accompany officers to the police station[183] "typically do not injure the physical person of the individual" but nonetheless "damage the individual's sense of . . . security."[184]

2. Psychological Safety Under Pervasive Surveillance

As facial recognition becomes ubiquitous, more intrusive surveillance is on the horizon and its psychological impact will be correspondingly greater. Today, stalking and individualized intimidation are in the main exceptional, not mass phenomena. Systemic tracing and retention of electronic communications is a mass phenomenon, but at least until recently it seems to have remained largely invisible to most people in the United States, Canada, and Europe. Similarly, while credit and other scoring systems are prevalent, their effects are concentrated in the economic sector. For a long time, credit scores were used primarily for

---

178. Brenda S. Sanford, *Stalking is Now Illegal: Will a Paper Law Make a Difference?*, 10 T.M. COOLEY L. REV. 409, 430 (1993) (quoting Rachel L. Jones, *His Obsession, Her Terror*, DETROIT FREE PRESS at 4H (Aug. 23, 1992)).

179. 470 U.S. 753, 762 (1985).

180. 470 U.S. 753, 762 (1985).

181. *Id.* at 761–62 (citing Payton v. New York, 445 U.S. 573 (1980)).

182. *Id.* at 762 (citing Katz v. United States, 389 U.S. 347 (1967)).

183. *Id.* (citing Dunaway v. New York, 442 U.S. 200 (1979)).

184. *Lee*, 470 U.S. at 762.

credit determinations.[185] More recently, landlords and employers have begun to use credit scores as inputs to their decision-making, and there have even been reports of dating applications matching by credit score.[186]

Current levels of surveillance and control are only the beginning. Much greater surveillance is coming. The Chinese government may currently be the world leader in its experiment with social scoring mechanisms,[187] but the use of "reputation mechanisms in law, regulations, and governance is not a uniquely Chinese phenomenon"; rather it "has been underway globally."[188] Privacy will achieve new salience when people begin to fear that every action they take both online and in person will be stored and scored. Whether everyone will react as if they were being stalked, or if mass observation and scoring will become a new normal, remains to be seen.

C. Protection of Spatial Privacy

Spatial privacy involves a person's interest in the privacy of particular physical locations, primarily those the person considers intimate.[189] The most common examples would be the expectation of privacy a person has in his or her own room, office, or home. Spatial privacy focuses on excluding unwanted intrusion or inspection in an area a person identifies as theirs. Often, spatial privacy is associated with the intimate relations or family life that occur in the home, such as peeping in a bedroom window.[190] The criminal procedure concept of a "reasonable expectation of privacy," and the Fourth Amendment's protection against unreasonable search and seizure, also originate from this privacy right.[191]

---

185. *See* Jonathan Weinberg, *'Know Everything that can be Known About Everybody': The Birth of the Credit Report*, 63 VILL. L. REV. 431, 434–35 (2018).

186. *Online Dating Site Matches Users by Their Credit Score*, CBSPHILLY (Apr. 5, 2017, 8:44 AM), https://philadelphia.cbslocal.com/2017/04/05/dating-credit-score/ [https://perma.cc/FU3X-QF9P]; *see also* Suzanne Wooley, *Your Credit Score Could Make or Break Your Love Life*, BLOOMBERG (Aug. 21, 2017, 2:00 AM), https://www.bloomberg.com/news/articles/2017-08-21/a-high-credit-score-can-make-you-look-sexy-on-dating-apps [https://perma.cc/PQ77-ZTAN] (reporting that financial responsibility "was ranked as a very or extremely important quality in a potential mate by 69 percent of the 2,000 online daters surveyed").

187. Xin Dai, *Toward a Reputation State: The Social Credit System Project of China* (June 10, 2018) (on file with Ocean University of China and Peking University Law School), *available at* https://ssrn.com/abstract=3193577 [https://perma.cc/3VMX-G7Q7].

188. *Id.* at 2; *see also* Lior J. Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667 (2008).

189. Koops et al., *supra* note 13, at 567.

190. *Id.* at 500.

191. *Id.* at 515–16.

D. Protection of Decisional Privacy

Decisional privacy consists of a person's interest in the privacy of personal decisions, primarily those relating to intimate relationships. Decisional privacy focuses on the idea that people should have the right to privacy regarding choices relating to sexuality, relationships, and family.[192] While we are not prepared to make or defend the claim that reproductive autonomy is an aspect of "privacy" as such, some examples cited by scholars include the right to make uncoerced choices about sexual orientation, contraceptive use, and abortion.[193] So understood, the value of decisional privacy is reflected in court decisions that protect family life and personal decisions from government intrusion; consider, for instance, *Roe v. Wade*,[194] *Griswold v. Connecticut*,[195] and the constitutionally guaranteed rights to a family's privacy.[196]

1. Avoidance of Shame (and Blackmail)

Decisional privacy is reduced to the extent one is subject to external pressures such as shame or blackmail. One significant, although perhaps sometimes dubious, aspect of privacy is that it protects against the observation of actions that may cause shame. Society appears to be of two minds on this point. On the one hand, there are actions that are both shameful and criminal, and the protection of these is no virtue. Other, legal, activities may be immoral and embarrassing or have painful consequences if discovered; for instance, having an affair that might cause a divorce if discovered. However, there is also a substantial class of (usually legal) actions that some or all people may find shameful to have observed, and for which society either tolerates or even supports the average person's desire to not have those actions observed. Examples of legal but don't-flaunt-it activities include sex (generally a public-order offense if done in public, but not in private) and defecation (which is why there commonly are doors on toilet stalls). Furthermore, there are still people who would not want their sexual orientation or religious or political beliefs to be known by others.

In each of these cases, the *Typology*'s overlay of informational privacy reflects its role in protecting intimate aspects of privacy by guarding not

192. *Id.* at 567–68.

193. *Id.* at 521.

194. 410 U.S. 113 (1973).

195. 381 U.S. 479 (1965).

196. Koops et al., *supra* note 13, at 521.

just against shame, a potentially painful emotion,[197] but perhaps also against blackmail. The more surveillance people are subject to, the more they will either have to conform their behavior to social norms[198] or the more they will have to risk either shame or demand for hush money.

E. Protection of Communicational Privacy

Communicational privacy involves a person's interest in restricting unwanted access to their communication with other individuals. Communicational privacy includes the protection of speech, documents, phone calls, and electronic communications such as emails or text messages.[199] In U.S. law, this privacy interest finds its most evident expression in the First Amendment's protections of speech, religious liberty, and the freedom of association, but, as described in this section, it is also reflected in other doctrines and practices. Which zone of privacy these communications protections fall into under the *Typology* ranges from the intimate to the public zones, depending on the correspondent, the subject, and the context.[200]

Governments today are increasingly regulating communications technology to require both traceability of communications and storage of metadata and even content by information intermediaries.[201] The consequence is that any user of email, web services, or cell phones must act as if they are being monitored. Worse, with data retention, the government's monitoring need not be in real time, but can be applied retrospectively for months or years. The consequences are potentially severe, and can lead to political repression—or self-censorship.[202] This is not controversial: in *Bartnicki v. Vopper*,[203] for example, both the majority and the dissent agreed that "privacy of communication is essential if

---

197. *See* June P. Tangney, *The Self-Conscious Emotions: Shame, Guilt, Embarrassment and Pride in* HANDBOOK OF COGNITION AND EMOTION 541 (Tim Dalgleish & Mick J. Power, eds., 2005); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1212–18, 1260 (1998) (noting that informational privacy helps individuals avoid the embarrassment that accompanies the disclosure of certain personal details).

198. *See* Margot Kaminsky & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 518 (2015).

199. Koops et al., *supra* note 13, at 524, 567.

200. We address evidentiary privileges below in section III.H. As noted there, many evidentiary privileges, such as the clergy-penitent privilege, can be characterized as protecting communications in the *Typology*'s semi-private zone.

201. *See, e.g.*, A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95, 97 (2017).

202. *See* Kaminsky & Witnov, *supra* note 198, at 518.

203. 532 U.S. 514 (2001).

[democratic] citizens are to think and act creatively and constructively" because fear of being monitored can inhibit the willingness to voice critical ideas.[204]

1. Shield Laws

The proliferation of shield laws for journalists in most of the states in the United States demonstrates that legislatures understand how privacy both enhances safety in the semi-private zone, and enhances liberty more generally.

Shield laws respond to a problem caused by the clash between the value of a public informed by journalists able to rely on confidential sources and the legal system's focus on acquiring information relating to legal violations. "The United States public consistently relies on press coverage of leaked material to hold government actors accountable for controversial operations."[205] Yet despite the strong protections of the First Amendment, when it comes to being required to testify in court, or before grand juries, reporters have no more right to refuse than any other citizen.[206] Consequently, at common law, it was not improper for a prosecutor to attempt to require a journalist to disclose a source who had revealed information about a crime, although journalistic ethics required that reporters nonetheless protect their sources, even at pain of being jailed for contempt for their failure to testify.[207]

Thirty-one U.S. states have chosen to temper this rule with so-called "shield laws" that create a legal privilege for journalists.[208] In seventeen

---

204. *Id*. at 533 (citation and internal quotation marks omitted); *id.* at 543 (Rehnquist, C.J., dissenting) (citation and internal quotation marks omitted). *See generally* RICHARDS, *supra* note 175.

205. Elizabeth L. Robinson, *Post-Sterling Developments: The Mootness of the Federal Reporter's Privilege Debate*, 95 N.C. L. REV. 1314, 1314 (2017).

206. Romualdo P. Eclavea, Annotation, *Privilege of Newsgatherer Against Disclosure of Confidential Sources or Information*, 99 A.L.R. FED. 3D Art. 37 (2018) ("Traditionally, a newsgatherer, in the absence of a statute or court rule to the contrary, has no privilege to conceal and may be compelled to disclose in a legal proceeding before a court, grand jury, or other governmental bodies, the confidential information or the identity of a confidential source of information obtained by him in his professional capacity.").

207. Joel G. Weinberg, *Supporting the First Amendment: A National Reporter's Shield Law*, 31 SETON HALL LEGIS. J. 149, 156–58 (2006).

208. *Id.* at 173. The U.S. Justice Department also has special guidelines requiring personal authorization from the Attorney General to subpoena a reporter. The guidelines state that such subpoenas should only be authorized after "all reasonable alternative attempts have been made to obtain the information from alternative sources[,]" and the Department has attempted to negotiate with the journalist. 28 C.F.R. § 50.10 (2019). The guidelines, however, are only advisory, not binding. *See* Branzburg v. Hayes, 408 U.S. 665, 707 n.41 (1972) (noting that guidelines need not be followed in all cases).

other states, the courts have judicially created a qualified privilege allowing reporters to protect their sources.[209] While these rules vary, and do not apply to federal investigations and prosecutions,

> [i]n almost all the jurisdictions, the reporter's privilege applies in the grand jury context. Over half of the state shield statutes render absolute a reporter's privilege not to disclose confidential sources, and in virtually all of the remaining state statutes, the standard for piercing the reporter's privilege is high, requiring more than simple relevance to the proceeding. State shield laws provide varying scopes of protection. In fourteen States, the state's highest court or an intermediate appellate court has recognized a reporter's privilege. Lower courts in three States have recognized a reporter's privilege. Only Wyoming and Hawaii have not adopted some form of reporter's privilege.[210]

Because "[r]eporters cannot function without confidential sources,"[211] and because the public has an interest in the free flow of information, U.S. state authorities—and in a much more limited fashion, federal ones too[212]—have recognized the importance of protecting the identity of those sources. Here, privacy serves the security of the sources—and, arguably, the long-run security of all participants in democracy who otherwise would have to subsist on an information diet even more tightly controlled by governmental authorities.

The reporter's privilege to protect confidential sources is now anchored in international law. In 2011, the United Nations Human Rights Committee adopted an interpretation of freedom of expression that included a journalistic privilege, as recognized in Article 19 of the International Covenant on Civil and Political Rights.[213] Prior to this

---

209. *See* Weinberg, *supra* note 207, at 173–75.

210. *Id.* (emphasis omitted). Hawaii subsequently enacted a shield law, but it lapsed in 2013. *See* Jack Komperda, *Hawaii Shield Law Will Expire After Lawmakers Unable to Reconcile Competing Bills*, REPS. COMMITTEE FREEDOM PRESS (May 3, 2013), https://www.rcfp.org/browse-media-law-resources/news/hawaii-shield-law-will-expire-after-lawmakers-unable-reconcile-compe [https://perma.cc/HH7K-FW7F].

211. Scott Neinas, *A Skinny Shield Is Better: Why Congress Should Propose A Federal Reporters' Shield Statute That Narrowly Defines Journalists*, 40 U. TOL. L. REV. 225, 227 (2008).

212. The U.S. Supreme Court has not recognized a reporter's privilege, with its only relevant pronouncement being the somewhat opaque result *in Branzburg v. Hayes*, 408 U.S. 665, 690 (1972), which held that journalists, like other citizens, have no immunity from grand-jury subpoenas. *Id.* However, "[m]ost federal circuits recognize a qualified journalist's privilege not to identify a confidential source." David Abramowicz, *Calculating the Public Interest in Protecting Journalists' Confidential Sources*, 108 COLUM. L. REV. 1949, 1949 (2008).

213. U.N. HUMAN RIGHTS COMM., INT'L COVENANT ON CIVIL AND POLITICAL RIGHTS, gen. cmt. 34, para. 45 (Nov. 29, 2011); *see generally* Edward L. Carter, *"Not to Disclose Information Sources":*

pronouncement, the European Court of Human Rights (on multiple occasions), the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia, and the Special Court for Sierra Leone had each recognized some form of reporters' privilege.[214]

2. Protection of Whistleblowers

In order to encourage people to report fraud and other violations of trust, U.S. law provides for a number of protections designed to safeguard the identity of informants known as whistleblowers. U.S. law also contains a large number of statutory prohibitions of retaliation against whistleblowers, for example prohibitions on firing an employee who reported an offense,[215] but, necessarily, those only apply if the person retaliating knows the identity of the whistleblower. These rules, like those protecting witnesses and informants in criminal cases, are designed to encourage the reporting of misdeeds by those with knowledge of the same while at the same time protecting the whistleblower from the danger of physical or economic retaliation.[216] A whistleblower protection scheme figured prominently in the revelation of the Ukraine scandal that set off a presidential impeachment investigation in October 2019.[217]

The clearest example of a statutory anti-retaliation policy may be the Securities and Exchange Commission's (SEC) program to encourage and reward whistleblowing. Pursuant to the Dodd-Frank Act,[218] the SEC

Journalistic Privilege Under Article 19 of ICCPR, 22 COMM. L. & POL'Y 399 (2017).

214. *See* Carter, *supra* note 213.

215. *See, e.g.*, 18 U.S.C. § 1514A (2012).

216. *See* Whistleblower 10949-13W v. Comm'r, 107 T.C.M. (CCH) 1475, 1475 (2014) ("Proceeding anonymously is necessary to protect the whistleblower's professional reputation, economic interests and personal safety."); Anonymous v. Comm'r, 127 T.C. 89, 94 (2006) (holding that risk of "severe physical harm" to taxpayer and taxpayer's family outweighed general public interest in knowing taxpayer's identity); U.S. Navy-Marine Corps. Court of Military Review v. Carlucci, 26 M.J. 328, 335 n.9 (C.M.A. 1988) (recognizing "the importance of encouraging and protecting whistleblowers" through preserving their anonymity); *see generally* U.S. Tax Ct. R. 345 ("A petitioner in a whistleblower action may move the Court for permission to proceed anonymously, if appropriate."); 15 U.S.C.A. § 78j-1 (West 2019) (requiring the audit committees of issuers of securities to implement internal procedures that facilitate and encourage "anonymous" whistleblowing by employees about "questionable accounting or auditing matters").

217. *See* Annie Karni & Nicholas Fandos, *Legal Team Says it Represents a Second Whistle-Blower Over Trump and Ukraine*, N.Y. TIMES (last updated Oct. 11, 2019), https://www.nytimes.com/2019/10/06/us/politics/second-whistleblower-trump-ukraine.html (last visited Mar. 9, 2020); Michael D. Shear, *Highlights: Whistle-Blower Complaint Goes to House as Ukraine Phone Call Gets Released*, N.Y. TIMES (last updated Sept. 26, 2019), https://www.nytimes.com/2019/09/25/us/politics/trump-impeachment.html (last visited Mar. 9, 2020).

218. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat.

offers whistleblowers[219] in the financial industry the prospect of monetary bounties[220] and the promise of confidentiality.[221] Subject to limited exceptions,[222] whistleblowers may require the SEC to protect their identity, and even keep confidential the information that the whistleblower reveals if such information can reasonably be expected to reveal the identity of a whistleblower if made public.[223] As one commentator put it, "[t]his is a very important protection for prospective whistleblowers" because otherwise not only their current job, but also their standing in their community and their future employment prospects, could be "ruined"—making the promise of confidentiality "more important than the monetary reward."[224]

Indeed, guaranteeing anonymity for whistleblowers

> allows individuals to come forward who would otherwise remain silent for fear of reprisals. In so doing it promotes the public welfare which may be subverted by abuses of power by government officials, or the public safety, which may be threatened by dangerous practices of private industry. It may also promote honesty and accountability among managers who know they will find it difficult to conceal their indulgences.[225]

Partly as a result of keeping whistleblowers' identities secret, the SEC's program has been very successful:

> The SEC whistleblower program has proved to be popular with

---

1376, 1841–49 (2010).

219. Exactly who should qualify as a protected "whistleblower" is a subject of debate. *See* Carmen Germaine, *9th Circ. Says Dodd-Frank Protects Non-SEC Whistleblowers*, LAW360 (Mar. 8, 2017, 3:17 PM), https://www.law360.com/articles/899680/9th-circ-says-dodd-frank-protects-non-sec-whistleblowers [https://perma.cc/CQU7-QDCS]. But the issue need not detain us here.

220. Alexander Hall, *Whistling Different Tunes: A Comprehensive Look at The Future of Whistleblowers under Dodd-Frank*, 86 UMKC L. REV. 681, 685 (2018). In order to be eligible for bounties, the information given to the SEC must have come from the relator's own knowledge, and not have been available from publicly available sources. Furthermore, the information has to be strong enough to substantially influence—or cause the agency staff to create—an investigation. *See* Ronald H. Filler & Jerry W. Markham, *Whistleblowers—A Case Study in the Regulatory Cycle for Financial Services*, 12 BROOK. J. CORP. FIN. & COM. L. 311, 314–15 (2018).

221. Hall, *supra* note 220, at 686. The SEC's rules also provide for protection against retaliation if the whistleblower's identity is revealed. *Id.* at 686–87.

222. *See* Exchange Act, 15 U.S.C. § 78u-6(h)(2)(B)–(C) (2012) (primarily dealing with criminal referrals, for example, to a grand jury).

223. *Id.* § 78u-6(h)(2); *see also* Hall, *supra* note 220, at 686.

224. Hall, *supra* note 220, at 686.

225. Frederick A. Elliston, *Anonymity and Whistleblowing*, 1 J. BUS. ETHICS 167, 172, 176 (1982) ("In many cases [whistleblowers] are fired or demoted, transferred to unattractive assignments or locales, ostracized by their peers and cast into psychological and professional isolation." (emphasis omitted)).

> tipsters. In fiscal year 2016, the SEC received over 4,200 whistleblower tips, a forty percent increase over the first year of the program which began in 2012. By extrapolating these figures, it appears that the SEC has probably received over 10,000 tips since the implementation of its whistleblower program. By June 2017, the SEC had awarded over $175 million in bounties to whistleblowers. Several of the SEC's bounty payments were in the millions of dollars, including awards of $83 million, $30 million, $22 million, $20 million, $17 million and $4 million.[226]

If nothing else, this suggests that privacy as safety has real value. Indeed, the whistleblower program received a backhanded compliment from Republican appointees to the SEC who recently proposed to weaken it by lessening the awards offered to people who disclose major widespread frauds.[227]

3. Encryption

Cryptography, skillfully employed, prevents the interception of communications—shared secrets—by unauthorized third parties; it also protects recorded secrets, such as diaries.[228] Both functions are key aspects of privacy.[229] As Kim Lane Scheppele explains,

> Without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons . . . . This does not mean that a person actually has to keep secrets to be autonomous, just that she must possess the ability to do so. The ability to keep

---

226. Filler & Markham, *supra* note 220, at 315.

227. Whistleblower Program Rules, 83 Fed. Reg. 34,702 (proposed July 20, 2018) (to be codified at 17 C.F.R. pts. 240, 249). The proposal increases the awards for disclosure of small retail fraud, but commentators (and the two dissenters in the three-to-two commission vote) described overall effect as designed to undermine the effectiveness of the program and potentially contrary to the enabling statute. *See, e.g.*, Nicholas Piwonka, *Proposed SEC Rule Will Hurt Whistleblower Program*, WHISTLEBLOWER PROTECTION BLOG (July 5, 2018), https://www.whistleblowersblog.org/2018/07/articles/dodd-frank-whistleblowers/proposed-sec-rule-will-hurt-whistleblower-program/ [https://perma.cc/88CT-2WYY] (discussing how decreasing the potential size of a payout may disincentivize whistleblowers); Yves Smith, *SEC Knifes Its Whistleblower Program*, NAKED CAPITALISM (July 9, 2018), https://www.nakedcapitalism.com/2018/07/sec-knifes-whistleblower-program.html [https://perma.cc/YB4Q-DVBG] (arguing that the amendments will severely undermine program by reducing incentive needed to persuade most potential whistleblowers to speak out).

228. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (1994); A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

229. KIM L. SCHEPPELE, LEGAL SECRETS 302 (1988).

> secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.[230]

Cryptography also enables strong electronic authentication, making impersonation and identity theft more difficult.[231] With the help of intermediaries such as providers of Virtual Private Networks (VPN), cryptography also makes online tracking more difficult.[232]

Thus, encryption can enable anonymous speech,[233] and contributes to the freedom of association[234] as well as to intellectual privacy.[235] To the extent that cryptography helps mask a user's location, there is also a link between communications privacy and physical privacy.[236]

Currently, U.S. residents remain free to use cryptographic protections, despite a twenty-five-year on-again off-again campaign by law enforcement and intelligence agencies to enact limits on strong cryptography in order to enhance the government's ability to acquire communications intelligence.[237] Indeed, encryption is an increasingly

---

230. *Id.* (footnote omitted).

231. *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996).

232. A VPN prevents tracking by the user's Internet service provider; unfortunately, many web-based Internet activities still create vulnerabilities via more elaborate tracking and tracing technologies such as supercookies, see, for example, Nicholas Jackson, *The Next Online Privacy Battle: Powerful Supercookies*, THE ATLANTIC (Aug. 18, 2011), https://www.theatlantic.com/technology/archive/2011/08/the-next-online-privacy-battle-powerful-supercookies/243800/ [https://perma.cc/LP4R-M6YD] and online 'fingerprinting', see Electronic Frontier Foundation, *Panopticlick*, https://panopticlick.eff.org [https://perma.cc/FXJ7-MBR4]. Phone-based internet activities also expose the user to any vulnerabilities introduced by the apps on their phones.

233. *See, e.g.*, A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 U. PITT. J. L. & COM. 395 (1996) (explaining how encryption allows individuals to communicate anonymously over the internet); Froomkin, *Anonymity*, *supra* note 56 (explaining how encryption works and how, by enabling anonymously speech over the internet, encryption enhances freedom of speech).

234. *See infra* section III.F.

235. *See supra* section III.B.

236. Koops et al, *supra* note 13 (noting that protection of informational privacy relating to personal data "is also a precondition to protecting the underlying physical privacy type").

237. *See* SUSAN LANDAU, LISTENING IN: CYBERSECURITY IN AN INSECURE AGE (2018); A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Crytopgraphic Key "Escrow*," 1996 U. CHI. L. F. 15 (1996); A. Michael Froomkin, *From Anonymity to Identification*, 1 J. REG. & SELF-REG. 121, 123–25, 129–31 (2015) [hereinafter Froomkin, *From Anonymity*]; Jim Baker, *Rethinking Encryption*, LAWFARE (Oct. 22, 2019), https://www.lawfareblog.com/rethinking-encryption [https://perma.cc/26GG-QB3F]; Joseph Marks, *The Cybersecurity 202: Attorney General Barr fires up the encryption debate* (July 24, 2019), WASH. POST, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/07/24/the-cybersecurity-202-attorney-general-barr-fires-

standard part of information and communications technologies: it's built into iPhones,[238] web browsers,[239] and is the default for popular web pages.[240]

F. Associational Privacy

Associational privacy involves the freedom to choose with whom one wishes to interact.[241] This form of privacy ordinarily involves multiple people; the right to associational privacy exists to guarantee social relationships outside the home, and the freedom of assembly.[242] Associational privacy can also refer to the expectation of privacy that groups have in protecting their information from outsiders, as well as the right to exclude people from their group.[243]

U.S. courts have long recognized the connection between privacy and the constitutional right to free association, itself a cornerstone of the viability of a liberal democracy. In the course of litigation designed to prevent the NAACP from operating a chapter in Alabama, the Alabama state government obtained an ex parte order directing the NAACP to produce, inter alia, records containing the names and addresses of all of its Alabama members.[244] In a unanimous opinion, the U.S. Supreme Court overturned the production order, noting that "immunity from state scrutiny of [the NAACP's] membership lists which the Association claims on behalf of its members is here so related to the right of [the NAACP's] members to pursue their lawful private interests privately and to associate freely with others in doing so as to come within the protection of the Fourteenth Amendment."[245] As the Court stated,

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of

---

up-the-encryptiondebate/5d3789a388e0fa1454f7fea1/ (last visited Mar. 9, 2020).

238. *See Why Default iPhone Encryption Isn't Enough*, VIRTRU, https://www.virtru.com/blog/iphone-encryption/ [https://perma.cc/5J6G-QNAY].

239. Adam Thompson, *Browser Updates Round-Up: Continuing the Push for HTTPS Everywhere*, HASHEDOUT (Oct. 8, 2019), https://www.thesslstore.com/blog/browser-updates-round-up-continuing-the-push-for-https-everywhere/ [https://perma.cc/8W2U-63WF].

240. *Id.*; Lawrence E. Hecht, *SSL Adoption Continues to Rise*, THE NEW STACK (Apr. 14, 2018), https://thenewstack.io/ssl-adoption-continues-to-rise/ [https://perma.cc/J6VY-TLMS].

241. Koops et al., *supra* note 13, at 568.

242. *Id.* at 572.

243. *Id.* at 501.

244. NAACP v. Alabama, 357 U.S. 449, 453 (1958).

245. *Id.* at 466.

> governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.
>
> . . .
>
> Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[246]

Further, the Court held that freedom to associate with organizations dedicated to the "advancement of beliefs and ideas" is an inseparable part of the Due Process Clause of the Fourteenth Amendment.[247]

Highlighting privacy's tie to physical safety, two years later, in *Bates v. City of Little Rock*,[248] the Supreme Court held that that disclosure of the NAACP's local branch's membership lists "would work a significant interference with the freedom of association of their members" because evidence indicated that identification of the members resulted in harassment and threats of bodily harm.[249]

Just as the right to meet in private is protected by the First Amendment, so too is the right to speak (or write) anonymously. The Supreme Court has repeatedly noted the existence of a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[250] Political speech receives the highest constitutional protection because it "occupies the core of the protection afforded by the First Amendment."[251] The Supreme Court has consistently upheld the right of dissidents and others to speak anonymously when they have a credible fear of retaliation for what they say. Thus, the Supreme Court has struck down several statutes requiring public disclosure of the names of members of dissident groups.[252]

---

246. *Id.* at 462. The Court did not hold that membership lists were absolutely privileged from disclosure but emphasized that the State had failed to make a sufficient case that it needed the information. *Id.* at 466.

247. *Id.* at 460.

248. 361 U.S. 516 (1960).

249. *Id.* at 523–24.

250. New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

251. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 346 (1995); *see also* Talley v. California, 362 U.S. 60 (1960) (holding ordinance that prohibited distribution of anonymous handbills unconstitutional).

252. *See* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations"); Shelton v.

The tie between identity protection and safety remains a theme in more modern decisions protecting the right to anonymous political and religious speech.[253] In *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*[254] the Supreme Court struck down a village ordinance requiring all door-to-door solicitors and canvassers—whether religious or commercial—to register with the village and to disclose their identities and the reason they wished to go door-to-door.[255] The Watchtower Bible and Tract Society (known also as Jehovah's Witnesses), a religious group that wished to go door-to-door in order to proselytize, challenged the ordinance as unconstitutional. The Supreme Court agreed, holding that the "breadth and unprecedented nature of this regulation" meant that it violated the First Amendment: "Even if the interest in preventing fraud could adequately support the ordinance insofar as it applies to commercial transactions and the solicitation of funds, that interest provides no support for its application to petitioners [or] to political campaigns . . . ."[256]

The ability to keep identifying information private when engaging in political activity—that is, the ability to communicate anonymously or pseudonymously—serves many ends.[257] One of them is that it protects the speaker from retaliation, as activists can face threats and also actual violence.[258]

Tucker, 364 U.S. 479, 485–487 (1960) (holding invalid a statute that compelled teachers to disclose associational ties because it deprived them of their right of free association).

253. *Talley*, 362 U.S. at 64–65 ("Persecuted groups and sects . . . have been able to criticize oppressive practices and laws either anonymously or not at all . . . due in part to the knowledge that exposure of the names of printers, writers[,] and distributors would lessen the circulation of literature critical of the government."); *see also* Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton, 536 U.S. 150 (2002); *McIntyre*, 514 U.S. at 342.

254. 536 U.S. 150 (2002).

255. *Id.* at 150.

256. *Id.* at 168.

257. *See* A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95 (2017); Froomkin, *From Anonymity*, *supra* note 237; Froomkin, *Anonymity*, *supra* note 56.

258. *See, e.g.*, Chantal Da Silva, *Florida School Shooting Survivors Receiving Death Threats Over Their Efforts To Tighten Gun Control*, NEWSWEEK (Feb. 26, 2018), http://www.newsweek.com/florida-school-shooting-survivors-death-threats-819484 [https://perma.cc/38BB-4JK8] (discussing an activist who received death threats after campaigning for gun control measures). Relatedly, strong privacy protections are important to protect against oppressive governments. Repressive regimes often target dissidents who are then imprisoned, tortured, and sometimes killed. In *Dep't of State v. Ray*, the Supreme Court held that the identities of certain Haitian emigrants must be kept private in part because of the risk that the Haitian government would retaliate and perhaps even inflict physical harm. 502 U.S. 164, 176–77 (1991) ("[D]isclosure of the unredacted interview summaries would publicly identify the interviewees as people who cooperated with a State Department investigation of the Haitian Government's compliance with its promise to the United States Government not to prosecute the returnees . . . . How significant the danger of mistreatment may now be is, of course,

G. Protection of Proprietary Privacy—Physical and Virtual

Proprietary privacy concerns the use of property to keep objects or information from others[259]: A purse conceals objects from others, as does keeping objects in the glove compartment of a car.[260] Fourth Amendment law ordinarily controls when the government can pierce the concealment a person has put around an object or a conversation, and that law relies greatly on the nebulous and contextual concept of "reasonable expectations." For example, U.S. law recognizes that when bringing a suitcase through the airport, its owner has an expectation of privacy relating to what is inside the luggage as against other travelers, but not as against airport security or customs agents legally authorized to inspect the luggage for dangerous materials or contraband.[261] A surprising amount of private law relating to privacy tracks, or is influenced by, the expectations considered reasonable under the Fourth Amendment. For example, to make out a claim for the tort of unreasonable intrusion a plaintiff must demonstrate he or she had "an objectively reasonable expectation of privacy in the place, conversation, or activity upon which the defendant allegedly intruded."[262]

Traditionally, proprietary privacy related to things, tangible chattels. However, proprietary privacy increasingly relates to intangibles, data, virtual things. Privacy is obviously an essential component to the safety of any account secured by a password. Accounts, such as online bank accounts, may also be secured by requiring a user ID or even two-factor authentication.[263] Failing to keep access credentials private exposes the account's owner to financial or other fraud.

Even those who use reasonable safeguards for their access credentials remain at risk of identity theft (ID theft), a form of fraud in which the attacker acquires the target's credentials and then impersonates the target

---

impossible to measure, but the privacy interest in protecting these individuals from any retaliatory action that might result from a renewed interest in their aborted attempts to emigrate must be given great weight.").

259. Koops et al., *supra* note 13, at 567.

260. *Id.*

261. *Id.* at 518.

262. *Privacy, Technology, and the California "Anti-Paparazzi" Statute*, 112 HARV. L. REV. 1367, 1370 (1999) (citing Shulman v. Group W Prods., Inc., 955 P.2d 469, 490 (Cal. 1998)).

263. In two-factor authentication, the user must supply a second proof of authorization in addition to the user/password combination. Common examples include a hardware token such as a key fob, a code from an app on a cell phone, or keying in a code sent by email or text to a registered address or phone number. *See What is 2FA?*, SECURENVOY, https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm [https://perma.cc/5SNQ-9TS9].

to gain financial advantage. ID theft is commonly used to get access to bank accounts, income-tax refunds (real or fraudulently claimed), credit cards, and health care.[264] The U.S. government gives thirteen pieces of advice to consumers about how to protect against ID theft. Of these, nine involve securing information or being more private, and four involve increased monitoring of credit reports and other information.[265]

ID theft can have devastating effects on its victims. The consequences can be financial,[266] leading to destroyed credit ratings and harassment by debt collectors.[267] A common type of ID theft involves fraudulently filing a false tax return on behalf of another, claiming that a refund is due, and having it sent to the thief's address. In 2014, the IRS may have paid out as much $3.1 billion in refund checks to victims of identity thieves.[268] But that number pales before the Justice Department's estimate that in the same year 17.6 million Americans older than sixteen had their personal information stolen, leading to total damages of $15.4 billion.[269]

In particularly severe cases, the ID theft can be life-threatening, in one case even leading to the victim being implicated in—and publicly linked to—an international assassination. Nicole McCabe was an Australian woman living in Israel when she heard a radio broadcast implicating her in the alleged Mossad-led assassination of Mahmoud al-Mabhouh in a Dubai hotel room. McCabe had never been to Dubai— and she had her passport. But while her passport had not been physically stolen, the

---

264. *Identity Theft*, USA.GOV (last updated Nov. 27, 2019), https://www.usa.gov/identity-theft [https://perma.cc/6BGS-3DBN].

265. *Id.* The advice to check one's credit reports has been criticized on the grounds that "making individuals responsible for protecting their identity and reputation by such means is akin to requiring them to leave their homes unlocked while suggesting they check with the local pawn shop to see if any of their things are fenced as stolen." Shostack & Syverson, *supra* note 55, at 137.

266. *Id.*

267. For example, in the fall of 2012, Alice Lipski stole Helen Anderson's financial mail, including old credit-card statements. Doug Shadel, *'She Stole My Life' – How Millions Fall Victim to Identity Theft*, AARP THE MAGAZINE (Oct./Nov. 2014), https://www.aarp.org/money/scams-fraud/info-2014/identity-theft-protection.html [https://perma.cc/UWM3-PKDJ]. Lipski then registered as Anderson for a credit-monitoring service intended to prevent ID theft—which exposed Anderson's complete credit history, revealing numerous canceled and inactive credit cards. *Id.* Lipski then reported the cards as lost or stolen, got new cards and new online account information safeguarded by new usernames, passwords, and security questions. *Id.* Since Lipski set them up, Anderson was locked out of the accounts in her name. *Id.* Lipski then charged over $30,000 in Anderson's name, and was only caught because she forgot her purse in a department store. *Id.* Inside were ten driver's licenses—each with a different name, but all with Lipski's picture. *Id.*

268. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-508, IDENTITY THEFT AND TAX FRAUD: IRS NEEDS TO UPDATE ITS RISK ASSESSMENT FOR THE TAXPAYER PROTECTION PROGRAM 14 (2016).

269. U.S. DEPT. OF JUSTICE, BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2014, at 7 (2015).

assassins had apparently forged a copy of it which contained all of her personal information and substituted the agent's picture for hers.[270] McCabe reportedly stated that she was "'terrified,'" had not slept, and was "worried for [her] health and . . . [her unborn] baby's health."[271]

ID theft violates criminal laws in most states, and also federal law. The Identity Theft and Assumption Deterrence Act makes it a federal crime to knowingly transfer or use, without lawful authority, "a means of identification of another person" intending to commit or assist "any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[272]

H. Privacy in Evidentiary Privileges

U.S. law recognizes a host of evidentiary privileges. Although all evidentiary privileges support communications privacy, different privileges also support intimate, associational and, sometimes, public privacy.

Privileges prevent the acquisition or admission of potentially relevant testimony in service of other social policies. Thus, the right against self-incrimination protects, among other things, the intellectual privacy of the suspect.[273] The right also protects the physical safety of the suspect by making it illegal for officials to force confessions.

The spousal privilege supports privacy in the *Typology*'s intimate zone. There are actually two spousal privileges. The first is a testimonial privilege that protects an individual from being forced to testify in criminal proceedings in which their spouse is a defendant.[274] In some states, but not in the federal system, this testimonial privilege even allows

---

270. David Murray, *'Assassin' Nicole McCabe Alone and Scared in a World of Lies, Spies and Killers*, THE DAILY TELEGRAPH (Feb. 26, 2010), https://www.dailytelegraph.com.au/assassin-nicole-mccabe-alone-and-scared-in-a-world-of-lies-spies-and-killers/story-e6freuy9-1225834931178 [https://perma.cc/3SDB-AR2G].

271. *Id.*

272. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. 105-318, 112 Stat. 3007 (Oct. 30, 1998) (codified at 18 U.S.C. § 1028 (2012)). In addition, the Theft Penalty Enhancement Act of 2004, Pub. L. 108-275, 118 Stat. 831 (July 15, 2004) (codified at 18 U.S.C. § 1028A (2012)), increased penalties for "aggravated" identity theft, requiring courts to impose additional sentences of two years for general offenses and five years for terrorism related offenses. *Id.* And, the Identity Theft Enforcement and Restitution Act of 2008 amends 18 U.S.C. § 3663(b) (2012) to clarify that restitution orders for identity theft cases may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated identity theft.

273. *See generally* NEIL RICHARDS, INTELLECTUAL PRIVACY (2015).

274. 2 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 5:39 (4th ed. 2013).

one spouse to prevent the other from testifying.[275] The second privilege protects the contents of confidential communications between spouses during their marriage from testimonial disclosure; this privilege is narrower as it only applies to confidential communications, but when it exists it applies in both civil and criminal matters.[276]

The long-recognized clergy-penitent privilege, under which priests and other religious figures do not have to disclose confessional communications from parishioners, supports both intellectual and associational privacy. The privilege exists to protect religious freedom and to foster and encourage spiritual relationships,[277] but in the U.S. its reach has been reduced by laws in many states that require disclosure of child abuse.[278]

Lawyer-client communications are generally privileged against disclosure in order to avoid discouraging people from seeking legal advice, but again the privilege is not absolute. Lawyers can disclose client information without the client's permission in a small number of special circumstances such as if lawyer seeks to prevent a serious future harm to a third party.[279] Even so, this privilege supports communications privacy, behavioral privacy, and even decisional privacy.

1. Protection Against Invidious Discrimination

The privacy that enables freedom from illegal discrimination also cuts across several of the zones set out in the *Typology*. It affects the public zone, since the search for employment, housing, or even credit is not exactly intimate. That said, once one is in possession of a house, that place and the human relations that take place in it might best be characterized as intimate; similarly, once one has the job, then the office and its relationships also might best be characterized semi-private. Arguably, since some forms of discrimination are race-based (although religion, age,

---

275. *Id.*

276. *Id.*

277. *See* Christine P. Bartholomew, *Exorcising the Clergy Privilege*, 103 VA. L. REV. 1015 (2017) (setting out the history of the privilege and then critiquing as largely unnecessary).

278. *See* F. Robert Radel, II & Andrew A. Labbe, *The Clergy-Penitent Privilege: An Overview*, GROELLE & SALMON, http://www.gspalaw.com/the-clergy-penitent-privilege-an-overview/ [https://perma.cc/DED3-6RU7].

279. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (AM. BAR ASS'N 1983) (listing circumstances when attorney may disclose client information); *see generally* Chris Clark, *Against Confidentiality? Privacy, Safety and the Public Good in Professional Communications*, 6 J. SOC. WORK 117, 131 (2006) (arguing that under a liberal rights theory approach, some measures of privacy protect autonomy of an individual but that professional obligations of confidentiality should sometimes give way to needs of wider public).

and national origin are also possibilities), one might consider the withholding of facts that may provoke discrimination to belong in the "bodily privacy" section of the Intimate Zone where Koops et al. place genetic privacy.[280]

Most U.S. anti-discrimination laws penalize the use of certain known but "protected" information to make (primarily economic) decisions. Thus, for example, in the classic housing-discrimination story, the landlord knows or suspects the race of the applicant, which is what motivates the landlord's refusal to rent an apartment to the individual. Prohibited discrimination is not primarily a privacy story—what motivates the discrimination is the absence of privacy: the economic actor knows a fact about the applicant or worker that society has decided is invidious if treated as a factor in decision-making. Of course, in many cases, especially in an ongoing employment relationship, masking the information that someone is a member of a protected class is not a practical option. But in the set of cases where the parties have yet to establish a face-to-face relationship, not divulging the personal characteristic at issue would be a solution to the discrimination problem since if the decider didn't know, for example, the race of the applicant, and also could not infer it reliably,[281] then perforce the decision would be race-neutral.

U.S. federal statutes make it an offense for employers to discriminate on grounds of age,[282] disability,[283] genetic information,[284] race or color,[285]

280. *See* Koops et al, *supra* note 13, at 569.

281. When evaluating paper applications U.S. employers discriminate against applicants with African-American sounding names. *See* Marianne Bertrand & Sendhil Mullainathan, *Are Emily and Greg More Employable Than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination*, 94 AM. ECON. REV. 991, 991 (2004) (finding "[w]hite names receive 50 percent more callbacks for interviews").

282. The Age Discrimination in Employment Act (ADEA), Pub. L. No. 90-202, 81 Stat. 602, (codified as amended at 29 U.S.C. §§ 621-24 (2012)), forbids age discrimination in employment against qualified persons who are age forty or older.

283. The Americans with Disabilities Act (codified as amended at 42 U.S.C. § 12100 *et seq* (2012) and the Rehabilitation Act, 29 U.S.C. § 794 (2012), prohibit discrimination against qualified but disabled applicants in employment.

284. Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. 110–233, 122 Stat. 881 (codified at 42 U.S.C.§ 2000ff, *et seq.* (2012)), prohibits genetic information discrimination in employment.

285. Title VII of the Civil Rights Act of 1964, Pub. L. 88-352, 78 Stat. 241 (Title VII) (codified as amended at 42 U.S.C. § 2000e *et seq.* (2012)).

religion,[286] national origin,[287] sex,[288] or pregnancy.[289] Similar laws ban discrimination on grounds of race or color, national origin, religion, or gender in other important economic relationships such as housing,[290] or access to credit.[291] The formal structure of these rules requires the actors to ignore some feature of the applicant even though it may literally be staring the employer, landlord, or lender in the face: As many have noted, the dominant trope in US anti-discrimination law is a legally mandated 'blindness' to certain facts.[292]

The problem with most of these rules, however, is that they are hard to enforce since bias can be difficult to detect and even harder to prove. When possible, it is far more efficient to mask the information that might lead to discrimination. The effect of adding some privacy to hiring is potentially significant. When, for example, orchestras began to use a screen to hide the identity of players auditioning for places, the number of women hired increased 30% according to a study that looked at hiring patterns from 1970 to the 1990s.[293] On the other hand, outside the context of economic relations, there can be circumstances in which masking information about a person's race, gender, or sexual orientation can lead to the perpetuation of stereotypes and other unwanted results.[294]

Many genetic characteristics other than race and gender that might lead

---

286. *Id*.

287. *Id*. In addition, the Immigration Reform and Control Act of 1986 (IRCA), Pub. L. 99-603, 100 Stat. 3359 (codified in scattered sections of 8 U.S.C.), makes it illegal for an employer to discriminate with respect to hiring, firing, or recruitment or referral for a fee, based upon an individual's citizenship or immigration status.

288. Lily Ledbetter Fair Pay Act of 2009, Pub. L. 111-2, 123 Stat. 5 (2009) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.).

289. The Pregnancy Discrimination Act (PDA), Pub. L. No. 95-555, 92 Stat. 2076 (1978) (codified as amended at 42 U.S.C. § 2000e(k)) forbids discrimination based on pregnancy in any aspect of employment.

290. The Fair Housing Act of 1968, Pub. L. 90-284, 82 Stat. 73 (codified as amended at 42 U.S.C. §§ 3601–3619), forbids discrimination in all aspects of residential-real-estate-related transactions, such as buying, selling, or renting a home.

291. The Equal Credit Opportunity Act (ECOA), Pub. L. 93-495, Title V, 88 Stat. 1500 (1974) (codified as amended at 15 U.S.C. §§ 1691-1691f), forbids credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or whether a person receives income from a public assistance program.

292. Robert C. Post, *The Logic of American Antidiscrimination Law*, *in* PREJUDICIAL APPEARANCES 1, 14 (Robert C. Post, ed. 2001) (citing Owen M. Fiss, *A Theory of Fair Employment Laws*, 38 U. CHI. L. REV. 235, 235 (1971)).

293. *See* Claudia Goldin & Cecelia Rouse, *Orchestrating Impartiality: The Impact of "Blind" Auditions on Female Musicians*, 90 AM. ECON. REV. 715, 738 (2000).

294. *See* Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1131, 1140–45, 1167–69, 1183–84, 1201–02 (2004).

to genetic discrimination by employers, insurers, and others are not visible without some kind of testing. The U.S. Genetic Information Nondiscrimination Act (GINA)[295] currently protects workers against genetic discrimination in employment and insurance, but does not cover many other areas, notably college athletics[296] and arguably schools more generally.[297]

The case that privacy enhances economic safety is easiest to make when the characteristics that might prompt invidious discrimination are not visible to the naked eye. Marital status, some ethnic origins, and many religious affiliations will not be visible to the observer, which is why we have rules forbidding lenders, employers, and landlords to ask questions about these characteristics.

Similar arguments apply to a range of life choices (with, again, a range of visibility) that could become occasions for discrimination. Privacy protects the economically vulnerable from being targeted due to sexual orientation, associations, or a decision to terminate a pregnancy.[298]

IV. PRIVACY GAPS

New technologies create opportunities for surveillance and control. Enhancing privacy rights is one logical response to these threats. So, while above we surveyed examples of U.S. law seeking to protect safety by ensuring privacy, in this Part we offer examples of gaps in such protections: areas where safety is threatened by a lack of privacy regulation.

We identify and discuss three representative technologies—the Internet of Things (IoT), social media, and connected cars—each of which reduce

---

295. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-223, 122 Stat. 881 (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.). *Cf.* Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710 (arguing that while GINA has failed to fulfill its purpose of improving attitudes toward genetic testing, it has achieved unanticipated success as an employee privacy statute).

296. *See* Heather R. Quick, *Privacy for Safety: The NCAA Sickle-Cell Trait Testing Policy and the Potential for Future Discrimination*, 97 IOWA L. REV. 665, 669–70, 683–86 (2012) (critiquing NCAA legislation requiring Division I schools to require student-athletes to either undergo sickle-cell trait testing or release the school from liability on grounds that this will expose students to danger of subsequent genetic discrimination in employment).

297. *See* Tyler Wood, *Genetic Information Discrimination in Public Schools: A Common-Sense Exception*, 49 U. PAC. L. REV. 309 (2018).

298. *Cf.* Jean V. McHale & June Jones, *Privacy, Confidentiality and Abortion Statistics: a Question of Public Interest?*, 38(1) J. MED. ETHICS 31, 33 (2012) ("The need to maintain patient confidentiality, both for women who have had terminations and for those who will have in the future, is of course paramount to good healthcare. This is undoubtedly highly sensitive information.").

personal privacy and thus expose people to new dangers. IoT and connected cars expose the user (and others within the home or the car) to surveillance and potential manipulation, or disclosure of intimate facts. With social media, people effectively spy on themselves, raising questions about what sort of regulation, if any, would protect their privacy, and thus their safety.

Each of the technologies surveyed in this Part threaten to restrict behavioral privacy. Behavioral privacy consists of an individual's freedom to move about without surveillance while in public. U.S. law tends to assume that the reasonable expectation of privacy in public is quite limited. Nevertheless, the law does regard as reasonable certain expectations of privacy while in public, such as not being stalked or invasively monitored.[299]

Whether or not it is reasonable to expect a degree of privacy in public, cameras are increasingly ubiquitous, creating a risk that someone is recording any and perhaps all behavior outside the home. The rise of social media means that photos—and tagging—can happen anywhere.[300] Rapid improvement of facial recognition software creates the danger that images can cheaply and reliably be linked to identities. Also, as discussed below[301] connected cars provide another avenue for tracking personal movement outside the home. Together these and other technologies risk substantially chilling the freedom of association, and behavioral privacy more generally.[302] Meanwhile, a person's online activities, especially but not only on social media, have a legal status little different from physically public activity, thus extending both public and private surveillance into the home. If and when social scoring[303] becomes more common, the effects on behavioral privacy will only become more significant.

A. Threats from the Internet of Things (IOT)

The Internet of Things (IoT) is shorthand for to the ability of everyday objects to connect to the Internet and to send and receive data.[304] Up to

---

299. Koops et al., *supra* note 13, at 568; *see also supra* section III.A.2.d (Protection from Stalkers).

300. *See infra* section IV.C.

301. *See infra* section IV.B.

302. *See* Moritz Büchi et al., *Chilling Effects of Profiling Activities: Mapping the Issues* (Apr. 28, 2019) (unpublished manuscript), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id =3379275 [https://perma.cc/7HNJ-LYKQ] ; Kaminsky & Witnov, *supra* note 198.

303. *See* Kaminsky & Witnov, *supra* note 198.

304. FTC, THE INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at i (2015).

two billion IoT devices are in use around the world, with more to come.[305] Dangers from the proliferation of IoT devices are as varied as the devices themselves, and often invisible to the user. IoT devices can phone home to the manufacturer, they reveal information to third parties, and also may be vulnerable to hacking.[306] "Light switches, cooking pans, stuffed animals, basketballs, headbands, water bottles, rectal thermometers, and more are now all connected to the Internet and our mobile devices."[307] As IoT devices seem set to permeate the home, work, and public spaces, they implicate all four of the *Typology*'s zones of privacy: personal, intimate, semi-private, and public.

The enabling of unauthorized access to the devices creates dangers that the intruder will instruct the device to do something harmful, although the instruction and the harm depend on the device's capabilities. Even though it is early days, it is reasonable to expect that, in the future, IoT devices also will create unpredictable new dangers because they are potentially long-lived, and thus will outlive their security model.[308]

Domestic IoT devices range from juicers to condoms[309] to voice-activated digital assistants to home automation systems.[310] IoT devices also proliferate well beyond the confines of the home, as we connect everything to the Internet and cloud storage. For example, smart cities rely on IoT-connected devices to enhance "environmental monitoring and analysis of data to prevent waste. For example, smart trashcans . . . use real-time data collection and alerts to trigger bin collection."[311]

One especially stark set of IoT-related physical dangers arises from

---

305. Sukhvir Notra et al., *An Experimental Study of Security and Privacy Risks with Emerging Household Appliances*, *in* 2014 IEEE CONFERENCE ON COMMUNICATIONS AND NETWORK SECURITY 79 (2014). However, "breathless predictions of market [size] should be taken with a grain of salt." Gilad Rosner & Erin Kenneally, *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*, *in* CENTER FOR LONG-TERM CYBERSECURITY WHITE PAPER SERIES 5 (June 7, 2018), https://ssrn.com/abstract=3320670 (last visited Mar. 9, 2020).

306. "[M]any IoT devices have long-standing, widely-known software vulnerabilities that make them prone to exploit and control by remote attackers." Nick Feamster, *Mitigating the Increasing Risks of an Insecure Internet of Things*, 16 COLO. TECH. L.J. 87, 88 (2017).

307. Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J. L. & TECH. 581, 582. "Japanese security researchers have already hacked an IoToilet, giving them the ability to flush and squirt water at people." *Id.* at 582–83.

308. *Id*. at 581 (noting that objects, like coffee pots and dolls, can last long after the standard life-cycle of software).

309. *See* Stefan Ducich, *These Walls Can Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment*, 16 DUKE L. & TECH. REV. 278, 280–81 (2018).

310. Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1192 (2017).

311. *Id*. at 1195 (giving example of "Big Belly Trash").

medical devices, such as insulin pumps,[312] pacemakers, and implantable cardiac defibrillators.[313] Although as far as we are aware, as of this writing, there are no publicly reported incidents of an implanted medical device being hacked to harm the patient, the prospect prompted the recall of 500,000 pacemakers in 2017 alone.[314]

Similarly, IoT devices in the body or in the home could be hacked to permit the acquisition and misuse of the owner's personal information, creating risks to personal safety, which again will vary with what the device knows and can sense about the user. Information acquisition alone still poses personal dangers as some devices will know the user's location while others will have credit-card or other financial data. Still others will allow an attacker to infer location. For example, devices with motion sensors and voice-activated smart-home devices will behave differently when persons are in the house, revealing location by inference.

Even in the absence of malfunction or hacking, the makers of IoT devices may design them to permit the collection and then use of personal information, habits, locations, and physical conditions. In turn, this information might be used to make credit, insurance, and employment decisions,[315] or, if acquired by the public sector, to make decisions about individuals' dangerousness, or to follow up on suspicion of criminal actions.[316] In 2017, VIZIO paid the Federal Trade Commission and the New Jersey Attorney General's Office $2.2 million for installing software that could collect users' viewing data in eleven million consumers' televisions without their consent or knowledge. VIZIO TVs appended specific demographic information to the viewing data, such as sex, age, income, marital status, household size, education level, home ownership, and home value; the company then sold the viewing and demographic information to third parties.[317]

---

312. *See J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking*, REUTERS (Oct. 4, 2016), https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/exclusive-jj-warns-patients-of-insulin-pump-cyber-bug-low-hacking-risk-idUSKCN12411L [https://perma.cc/KR47-D9NR].

313. *See* Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things*," 2017 U. ILL. L. REV. 415, 436 (2017); Lily H. Newman, *Medical Devices Are the Next Security Nightmare*, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare/ [https://perma.cc/6P29-7XPJ].

314. *See* Nicholas Shields, *The FDA Has Recalled About 500,000 Internet-Connected Pacemakers Over Hacking Fears*, BUS. INSIDER (Sept. 1, 2017), http://www.businessinsider.com/fda-recalls-500000-internet-pacemakers-hacking-fears-2017-9 [https://perma.cc/QL48-FFL5].

315. *See* FTC, *supra* note 304, at ii.

316. *See* Andrew G. Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017) (discussing the emerging use of predictive policing).

317. Press Release, Federal Trade Commission, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without

Perhaps the most notorious recent IoT incident involved a Portland, Oregon couple who discovered that their Amazon Alexa device had somehow recorded a domestic conversation and then silently emailed the recording to an acquaintance.[318] Amazon described the incident as the result of multiple misheard commands, suggesting it was a rare and unusual event,[319] but it serves well as a proof of concept for how an IoT device can be listening in the home and quietly sending audio to anyone.

We probably have only just begun to imagine the ways in which hacked IoT devices can harm users. Already, domestic-abuse victims have reported that former partners used remotely controlled devices to change electronic locks, ring the doorbell, change the behavior of thermostats or lights, set smart speakers to blare music, or spy on them via security cameras.[320] In extreme cases, victims have been referred for involuntary psychiatric evaluation when they complained that their ex-partners were remotely controlling devices in their homes, or spying on them at all hours. "[Y]ou can start to look crazy," said the director of a Silicon Valley domestic-violence program.[321]

B. Threats from Connected Cars

Connected cars have some ability to record, send, or receive information.[322] How much varies with the vehicle and with time—newer cars tend to collect more information about the car's usage and location, the driver's behavior, and even non-automotive information such as a passenger's synced cell-phone contacts or messages.[323]

A connected car does not have to have any autonomous capabilities; conversely, autonomous vehicles almost certainly will require the ability

---

Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it [https://perma.cc/PV9X-FSKJ].

318. Ry Crist, *Alexa Sent Private Audio to a Random Contact, Portland Family Says*, CNET (May 24, 2018), https://www.cnet.com/news/alexa-sent-private-audio-to-a-random-contact-portland-family-says/ [https://perma.cc/UV85-7MM6].

319. *Id.*

320. *See* Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html (last visited Mar. 9, 2020); Catalin Cimpanu, *Someone Is Taking Over Insecure Cameras and Spying on Device Owners*, BLEEPINGCOMPUTER (June 23, 2018), https://www.bleepingcomputer.com/news/security/someone-is-taking-over-insecure-cameras-and-spying-on-device-owners/ [https://perma.cc/S9R6-Y5SP].

321. Bowles, *supra* note 320 (quoting Ruth Patrick, head of WomenSV).

322. LindseyBarrett, *Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception*, 106 GEO. L.J. 181, 184 (2017).

323. *Id.* at 185.

"to collect, send, and receive different types of data, or will at least depend on some manner of mapped data (such as through GPS) for the vehicle to function autonomously, in addition to any connected features the car may have."[324]

Thus, the car of the future, and some of the cars of today also, will be able to store and report not just the vehicle's location and speed, but also the passenger's media habits, cell-phone calls, and even in-car conversations. Already today, connected-car systems come standard in many models; not only are they active whether or not the user chooses to use them but even a determined hobbyist willing to void the warranty may find them hard to disable.[325] Connected cars can also be very invasive. While yesterday's drivers could reasonably think of their in-car time as a private moment, today's BMWs come with Alexa built-in,[326] and perhaps listening in as well.[327] Other cars may soon have sensors capable of voice or facial recognition of all passengers, allowing tailoring of the driving experience to their preferences and health monitoring of drivers, but also collection of yet more information about the car's use.[328] Manufacturers may include an off switch—the VW Golf has a little-known switch only accessible to dealers that can turn off data sharing[329]—but no U.S. law requires that the car makers do so.[330]

---

324. *Id.* at 187–88.

325. Shuko, *How to kill CarNet (also, what's inside the box and buttons*.), GOLFMK7 (April 20, 2015), https://www.golfmk7.com/forums/showthread.php?t=9618 [https://perma.cc/3CVR-HE7G] ("Just removing the antenna did not disable the communications. It [a VW Golf] was able to connect as if nothing was wrong, even after I tried shorting the leads together.").

326. Frederic Lardinois, *BMW's Alexa Integration Gets it Right*, TECH CRUNCH (July 29, 2018), https://techcrunch.com/2018/07/29/bmws-alexa-integration-gets-it-right/ [https://perma.cc/733V-DRVE].

327. Erin Biba, *How Connected Car Tech is Eroding Personal Privacy*, BBC (Aug 9, 2016), http://www.bbc.com/autos/story/20160809-your-car-is-not-your-friend [https://perma.cc/F4FG-8WGZ].

328. Future of Privacy Forum, *The Connected Car and Privacy: Navigating New Data Issues* 8 (Nov. 13, 2014), https://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf [https://perma.cc/WLQ5-SUYE].

329. Biba, *supra* note 327.

330. In 2014, U.S. automakers voluntarily subscribed to a set of "Consumer Privacy Protection Principles" promising transparency as to their monitoring activities. However, under these principles when a participating automaker provides adequate notice to the consumer, the "Owner's or Registered User's acceptance and use of Vehicle Technologies and Services constitutes consent to the associated information practices." In other words, the consumer need give no further affirmative consent. The sole exceptions requiring actual affirmative consent are the use of geolocation information, biometrics, or driver information for marketing, or the sharing of any of these three types of information with third parties. ALLIANCE OF AUTO. MFRS., INC. & ASS'N OF GLOBAL AUTOMAKERS, INC., CONSUMER PRIVACY PROTECTION PRINCIPLES: PRIVACY PRINCIPLES FOR VEHICLE TECHNO LOGIES AND SERVICES 8 (2014), https://autoalliance.org/wpcontent/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf [https://perma.cc/B4PB-2Z57].

The connected car will mate the dangers of location tracking with the dangers of the IoT, making a person's location more visible to attackers, and also putting the car at some risk of being hacked in ways that might endanger the passengers. In so doing, connected cars implicate the *Typology*'s intimate zone (special privacy), the semi-private zone (not only communications privacy but also associational privacy, in that the car will allow third parties to use location mapping to reveal associations), and the public zone (in that its tracking powers effect behavioral privacy).

C. Threats from Oversharing

Lack of privacy—usually self-inflicted via social-media posts—has created new dangers for social media users. Instagram posts can reveal details about the home and about children. Twitter routinely geo-tags posts made from cell phones, revealing the poster's location.

Consider the threat that social media posts can pose to travelers. "'Instead of looking for physical signs that a home is unoccupied, burglars can simply scan Instagram posts, monitor Twitter feeds and check Facebook for signs that someone isn't home.'"[331] Posted photos showing off prized items within one's home can become personalized treasure maps for burglars.

Posting the wrong picture may also obviate the need for would-be intruders to break in. A photo clearly depicting a house or car key can provide sufficient detail for an intruder to make a usable copy of the key,[332] leading one commentator to call on journalists to "Stop Posting Photos of Real Keys in News Stories."[333] A similar problem arises when news or other photos taken in offices or homes reveal passwords on strategically placed post-its. Notoriously, a photo of the Hawaii Emergency Management Agency—taken shortly after the false missile alert that briefly terrified residents of that State—revealed a password for accessing the alert system.[334]

Although oversharing implicates privacy interests in arguably all four

---

331. *The Hidden Dangers of Oversharing on Social Media*, GREATER NASHVILLE HOUSE & HOME & GARDEN, (Jan. 31, 2018), https://houseandhomenashville.com/5571/the-hidden-dangers-of-oversharing-on-social-media/ [https://perma.cc/D7L2-CJAC] (quoting Mercury Insurance VP of Claims Kevin Quinn).

332. Schuyler Towne, *A Key You Can Photograph Is a Key That Can Be Copied*, GIZMODO (Feb. 13. 2014), https://gizmodo.com/any-key-you-can-photograph-is-a-key-that-can-be-copied-1522264272 [https://perma.cc/FUP2-JP47].

333. *See* Brady Dale, *Stop Posting Photos of Real Keys in News Stories*, OBSERVER.COM (May 5, 2016), http://observer.com/2016/05/copying-keys-from-photos/ [https://perma.cc/94LV-L6YR].

334. *See* Kif Leswing, *A Password for the Hawaii Emergency Agency was Hiding in a Public Photo, Written on a Post-It Note*, BUS. INSIDER (Jan. 16, 2018), http://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1 [https://perma.cc/D8UV-D5LN].

zones, it differs from our two other examples in key respects. First, oversharing is something that people do to themselves. Second, the communication, if not necessarily all the meta-data that gets associated with it, is voluntary and is constitutionally protected speech on the part of the social media user. As a result, even if some uses of social media may put the user in danger, the scope for regulation is very limited, and may not extend beyond user education campaigns and transparency rules requiring social media platforms to disclose what sort of invisible information they may collect or disclose.

CONCLUSION

As we stated at the outset, privacy is not a one-way street. We do not dispute that in many cases transparency—the absence of privacy—can enhance safety. Instead, we have sought to demonstrate that privacy too can enhance various types of safety, and that indeed current law and social institutions frequently recognize and cater to this reality.

As our survey in Part III shows, how and when privacy is safety varies with the circumstances. Some privacy protections, especially those that protect against physical dangers, are direct, but many are mixed in with larger social goals. We protect informants and whistleblowers for reasons much the same as we protect penitents and political organizers: in each case, we think that by making people safe we not only protect the individual but serve a broader social policy.

In both law and philosophy, claims to privacy require justification. Some classic justifications are based on first principles, claiming that privacy is itself a fundamental human right. For example, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and many other international and regional treaties recognize privacy as fundamental.[335]

But justifications can also rely on instrumental claims that privacy furthers worthy goals, which themselves trace their provenance to something fundamental. Instrumental claims for privacy come in many forms, ranging from Richard Posner's claim that privacy is no more than an intermediate good (and thus, actually, quite often a bad) to empirical claims that privacy is an essential component of human flourishing and self-determination because it creates a zone of mental or physical independence necessary to allow experimentation and self-realization. In between these extremes lie practical accommodations—many of which

335. *See* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 MARSHALL. J. COMPUTER & INFO. L. 1, 3 (1999).

we may take for granted. Not surprisingly, though, instrumental justifications always relate to a person's interactions with social practices.

In general, these instrumental arguments are subject to two types of counterarguments. First, they can be rebutted by countervailing instrumental arguments: each claimed good effect can be offset by a claimed equal or larger harmful effect. Second, if rights are trumps,[336] then instrumental claims may be vulnerable to pure rights-based claims, although the extent to which that is convincing may depend on how central the specific instrumental claim is to the realization of the underlying right or rights that it serves, enhances, or enables.

Despite our recognition of these potential rebuttals, we have focused here on instrumental cases for understanding privacy as safety because those are the ones most likely to persuade U.S. administrative agencies to regulate with any eye toward protecting privacy as part of their variegated missions to protect people against various risks.[337] If the United States had a general privacy policy akin to the GDPR, then such arguments would be unnecessary because U.S. agencies would have a broad freestanding obligation to consider privacy for its own sake rather than privacy as something else. Yet even without such a general mandate, U.S. law contains many provisions designed to enhance and protect public safety. If privacy is safety, even only in part, then U.S. law may turn out to be more protective of privacy than any of us suspected.[338]

Nevertheless, there are still areas where regulation could increase safety by increasing privacy. If privacy has instrumental value because it protects safety, for instance, if it is safety, then when new technologies undermine privacy in ways that threaten safety directly or indirectly, agencies with safety mandates will have the duty, or the discretion, to intervene. And even where regulation might be inappropriate or difficult, as with the case of oversharing, we would benefit from a better understanding of the ways in which the absence of privacy causes an absence of safety.

By showing that privacy, in several of its varied forms, enhances safety, we have tried to underline how privacy has far broader safety effects than is commonly recognized. We hope this will spur greater respect for the instrumental value of privacy, more privacy protections in the United States, and in turn more safety.

---

336. *Cf.* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY, at xi (1977).

337. As noted above, a future work, tentatively titled "Safety as Privacy," will seek to show that privacy falls within the safety mission of several U.S. administrative agencies.

338. *Cf.* MOLIERE, LE BOURGEOIS GENTILHOMME, Act II; scene 6 ("*Par ma foi! il y a plus de quarante ans que je dis de la prose sans que j'en susse rien.*") (emphasis in original) (translated into English as: "*By my faith! For more than forty years I have been speaking prose without knowing it*").